Universidade de Lisboa
Faculdade de Ciências
Departamento de Estatística e Investigação Operacional

Metodologias de Avaliação Operacional do Risco de Segurança na Proteção de Portos

Leandro da Silva Teixeira

Doutoramento em Estatística e Investigação Operacional

Especialidade de Análise de Sistemas

2015

Universidade de Lisboa
Faculdade de Ciências
Departamento de Estatística e Investigação Operacional

Metodologias de Avaliação Operacional do Risco de Segurança na Proteção de Portos

Leandro da Silva Teixeira

Tese orientada pelo Prof. Doutor António José Lopes Rodrigues,
especialmente elaborada para a obtenção do grau de doutor em
Estatística e Investigação Operacional,
especialidade de Análise de Sistemas

2015

A minha esposa, Maria, pelo apoio absoluto, paciência, incentivo e momentos de paz.

Amo-te!

A meus filhos, Camila e Artur, razões de meu viver.

Este momento faz parte de nossa história!

AGRADECIMENTOS

Ao meu orientador, Prof. Dr. António José Lopes Rodrigues, pelo qual eu tenho a mais alta estima, agradeço toda a confiança depositada, dedicação e apoio prestado durante minha estada em terras lusas.

Aos professores e funcionários do CIO, em especial a Prof. Dra. Maria Eugénia Captivo, pelo apoio e agradável convivência.

Ao Prof. Dr. José Luís Nunes do Carmo, toda a colaboração e disponibilidade para discutir as melhores formas de apresentação desta tese.

Aos colegas de investigação do projeto SAFEPORT, Diogo e João, pelo valioso apoio nas minhas dúvidas relacionadas com o uso do MATLAB.

À amiga Patrícia, os esclarecimentos pertinentes às diferenças entre a "língua portuguesa do Brasil" e a de Portugal.

À Marinha do Brasil, o apoio financeiro e a oportunidade de ter sido aluno da Faculdade de Ciências da Universidade de Lisboa!

Por fim, o meu profundo e sentido agradecimento a todas as pessoas que contribuíram para a concretização desta tese, estimulando-me intelectual e emocionalmente.

RESUMO

Os portos são alvos potenciais para ataques terroristas devido à importância que representam para a economia e para a sociedade. Nesta tese, apresenta-se uma metodologia para apoiar o processo de decisão no planeamento de recursos para a vigilância e proteção de portos contra ameaças terroristas. Centramos a preocupação, sobretudo, na possibilidade de ataques por via marítima, seja à superfície, seja abaixo da linha de água.

Sob o nosso ponto de vista um sistema de apoio à decisão pode produzir soluções estratégicas de custo-benefício razoável, com recomendações para a proteção, se for apoiado por uma forma mais confiável de avaliação do risco de segurança. Sendo assim, a alocação de recursos de proteção pode ser apoiada por uma metodologia baseada na adaptação de uma técnica empregada em âmbito militar denominada Avaliação Operacional (AO). O principal objetivo da AO é reduzir o risco de um equipamento/sistema não satisfazer a expectativa do utilizador, considerando custo, aspetos cognitivos, doutrina, táticas, vulnerabilidades e tipos de ameaças.

Assim, o risco de segurança é aqui definido por índices georeferenciados que descrevem a distribuição espacial de valores desse risco. Esses índices são estimados a partir de dados objetivos, sendo também incorporadas as perceções subjetivas dos agentes de decisão envolvidos.

A administração de um porto pode envolver um elevado número de *stakeholders* no planeamento das medidas de proteção perante tais ameaças. Assim, considerámos a oportunidade de desenvolver duas propostas para agregar as opiniões de um grupo. A primeira consiste num novo método de elicitação e agregação de opiniões de um grupo, cuja resposta, uma função de densidade de probabilidade, pode ser interpretada como uma representação do estado de incerteza e multimodalidade dos agentes de decisão envolvidos. A segunda proposta refere-se à agregação das funções de utilidade de um grupo por meio da média geométrica dos parâmetros de aversão ao risco das funções de utilidades individuais.

Palavras-chave: Risco de segurança; Elicitação e agregação de opiniões; Estimação de densidades; Funções utilidade; Aversão ao risco**.**

ABSTRACT

We present a methodology to support the planning of what resources should be allocated, and where and how they should operate to provide adequate protection of ports from terrorist threats originating from the waterside, below or above the sea surface.

A decision support system can produce reasonable cost-effective strategy solutions, with recommendations for protection, if supported by a reliable form of security risk assessment. Therefore, the allocation of resources for protection can be supported by a methodology based on the adaptation of a technique employed in the military area named Operational Analysis (OA). The main objective of OA is to reduce the risk of an equipment or system not satisfying the user expectations, considering cost, cognitive aspects, doctrine, tactics and types of threats.

Therefore, security risk is here defined by georeferenced indexes that describe the spatial distribution of that risk. Those indexes are estimated from objective data, while also embedding the subjective perceptions of decision-makers.

A port administration may involve a large number of stakeholders in the planning of the protection measures against such threats. Thus, we considered the opportunity to develop two proposals for aggregating opinions within a group. The first one consists of a new method for the elicitation and aggregation of group opinions, whose output, a probability density function, can be interpreted as a representation of the state of uncertainty and multimodality of the decision agents involved. The second proposal is focused on the aggregation of the utility functions of the group members by computing the geometric mean of the risk aversion parameters of the individual utility functions.

Keywords: Security risk; Elicitation and aggregation of opinions; Density estimation; Utility functions; Risk aversion.

ÍNDICE

LISTA DE FIGURAS

Figura

LISTA DE TABELAS

Tabela

LISTA DE SIGLAS E ACRÓNIMOS

AIS	*Automatic Identification System*
AO	Avaliação Operacional
AOC	Aspetos Operacionais Críticos
AoI	*Area of Interest*
DoD	Departamento de Defesa dos EUA
EC	Equivalente certo (método)
F.d.p.	Função (de) densidade de probabilidade
FMECA	*Failure Mode and Effects Criticality Analysis*
FMEA	*Failure Mode and Effect Analysis*
USCG	Guarda-Costeira dos EUA
IED	*Improvised Explosive Device*
ISPS	*International Ship and Port Facility Security*
MBRA	*Model-Based Risk Assessment*
MSRAM	*Maritime Security Risk Analysis Model*
NATO	*North Atlantic Treaty Organization*
NIPP	*National Infrastructure Protection Plan*
PERT	*Program Evaluation and Review Technique*
PRA	*Probabilistic Risk Analysis*
RAMCAP	*Risk Analysis and Management for Critical Asset Protection*
SSR	*Spatial Security Risk*
SSRI	*Spatial Security Risk Index*
TRAM	*Transit Risk Assessment Tool*
USS	*United States Ship*
VTS	*Vessel Traffic System*

1 INTRODUÇÃO

1.1 CONSIDERAÇÕES INICIAIS

Os portos possuem inúmeras instalações que podem ser usadas como alvos de ameaças terroristas, incluindo navios e bases militares, navios de cruzeiro, terminais de passageiros, terminais de carga e até mesmo áreas de lazer. Sob o ponto de vista histórico este fenómeno é pouco relevante. Até a presente data, podemos citar os ataques ocorridos em março de 2004, onde mergulhadores do *Hamas* atacaram uma instalação israelita de vigilância costeira, e em abril do mesmo ano, instalações de petróleo na costa do Iraque sofreram ataques terroristas similares. A Marinha do Sri Lanka perdeu alguns navios em 1995, quando os *Tigres Tamil* usaram mergulhadores suicidas para atacá-los. A mais conhecida ação terrorista marítima teve lugar no porto do Iémen contra o *USS Cole* no ano 2000, que contabilizou 17 marinheiros mortos como resultado da ação terrorista.

Contudo, é imprudente menosprezar o estado atual da ameaça terrorista marítima contra os portos com base em dados históricos, visto que no passado as táticas empregadas nesse tipo de terrorismo não se constituíam como efetivas, muito se devendo a falta de capacidade dos agentes. Entretanto, um ataque terrorista contra um porto pode causar impactos de longo prazo. Citamos como exemplo, o porto de Paranaguá no Brasil que possui uma área de influência de mais de 800.000 km^2, compreendendo o Estado do Paraná e parte dos estados de São Paulo, Santa Catarina, Rio Grande do Sul, Mato Grosso, Mato Grosso do Sul e Rondônia. Inclui também o Paraguai, que dispõe de um entreposto de depósito franco no porto. Pesquisas revelam que a economia mundial depende do comércio marítimo, que assegura cerca de 80% do transporte de mercadorias do comércio mundial. Desta forma, menosprezar este cenário pode ser imprudente.

Desde os atentados de 11 de setembro de 2001, envolvendo o sistema de transporte aéreo dos EUA, diversos mecanismos foram introduzidos e várias pesquisas foram desenvolvidas com o objetivo de reduzir a vulnerabilidade de **infraestruturas consideradas críticas** para esse tipo de ameaça. A provisão de segurança contra ameaças intencionais passou a ter maior importância nas análises de decisão sobre os investimentos e alocação de recursos.

Como elementos críticos desses quadros de referência, os custos adicionais estimados para a alocação de medidas de segurança mais severas redirecionaram o foco das análises para a comparação do custo total dos investimentos em segurança tendo em conta os benefícios esperados, incluindo, nessa comparação, as **estimativas dos riscos de segurança associados**. Logo, uma avaliação dos riscos envolvidos acabou emergindo naturalmente como estratégia relevante para a provisão da segurança contra ameaças intencionais.

Entre as medidas regulamentares que foram aprovadas e implementadas multilateralmente no contexto desse problema inclui-se o Código Internacional para a Proteção de Navios e Instalações Portuárias — Código ISPS (IMO, 2003). Constitui-se como o elemento central perante as preocupações com as ameaças terroristas no ambiente marítimo e, consequentemente, a proteção de portos. Este código tem por objetivo o estabelecimento duma moldura internacional para a cooperação entre os estados que envolva os governos, empresas de navegação e administrações portuárias de forma a identificar ameaças e tomar as devidas medidas preventivas. Realça-se como uma das medidas estabelecidas o facto que todo o governo contratante deve assegurar a execução de uma avaliação de proteção das instalações portuárias. Esta é fundamentalmente uma **avaliação de riscos** de todos os aspetos de operação de uma instalação portuária a fim de determinar quais as partes mais suscetíveis, e/ou onde é mais provável de ocorrer um ataque.

De acordo com o Código ISPS, a avaliação da proteção das instalações portuárias deverá incluir, pelo menos, os seguintes elementos:

- Identificação e avaliação de bens móveis e infraestruturas relevantes, que seja importante proteger;
- Identificação de possíveis ameaças a bens móveis e infraestruturas e a probabilidade da sua ocorrência, a fim de estabelecer e prioritizar medidas de proteção;

— Identificação, seleção e prioritização de contramedidas e alterações nos procedimentos e seu nível de eficácia quanto à redução de vulnerabilidade;
— Identificação de fraquezas, incluindo fatores humanos, na infraestrutura, planos de ação e procedimentos.

Contudo, um porto é uma infraestrutura complexa com acessos por via marítima e terrestre, conectado com outros modais de transporte e localizado, geralmente, próximo de centros urbanos, proporcionando diversas vias de acesso a agentes terroristas, seja por terra ou por mar. Este problema de segurança é normalmente investigado apenas em cenários militares, onde há diferentes possibilidades de agir e reagir contra uma ameaça e onde o tráfego do porto é rigidamente controlado. Nos portos civis os problemas são radicalmente diferentes, uma vez que o tráfego não é totalmente controlado, há menos possibilidades para testar a segurança do porto de uma forma eficaz e cada navio pode ser um possível alvo.

Outra característica relevante à problemática da proteção de um porto, diz respeito à multidisciplinaridade que se vê refletida no alargado número de autoridades, *stakeholders* envolvidos. No caso português, de acordo com Decreto-Lei nº 226/2006 temos:

— O Instituto Portuário e dos Transportes Marítimos;
— A Autoridade Marítima Nacional;
— As capitanias dos portos;
— As administrações portuárias;
— A Polícia Judiciária;
— O Serviço de Estrangeiros e Fronteiras;
— A Autoridade Nacional de Saúde;
— A Polícia de Segurança Pública; e
— A Guarda Nacional Republicana.

Já para o Brasil, o Decreto nº 1507/2002 define as competências e as autoridades envolvidas na segurança dos portos brasileiros:

— Departamento da Polícia Federal;
— Capitania dos Portos;
— Secretaria da Receita Federal;
— Administração Portuária; e
— Governo do Estado onde está localizado o porto.

A complexidade das variáveis de decisão e a natureza incerta de possíveis ameaças, bem como a necessidade de providenciar uma base defensável para a alocação de recursos para a proteção de um porto onde diversos decisores estão envolvidos é um importante e desafiante problema. Para o estabelecimento de qualquer processo de avaliação de riscos, as perguntas e questões que requerem a atenção dos tomadores de decisão precisam de ser identificadas. A natureza dessas questões deve levar a uma estrutura matemática adequada à utilização, de modo a proporcionar resultados a uma gestão eficaz do processo de tomada de decisão sob incerteza.

Precisamente nesse sentido surgiu o projeto SAFEPORT (Martins *et al.*, 2010) no âmbito do programa da NATO para a proteção de portos contra ameaças terroristas. O projeto destina-se a conceber, implementar e testar um sistema de apoio à decisão para proteção de portos a partir de possíveis **ataques terroristas originados em meio marítimo**, quer em tempo de paz, quer em cenários de conflito. O seu objetivo principal é o desenvolvimento de um sistema de apoio à decisão capaz de produzir recomendações para as configurações de recursos que permitam fornecer uma vigilância e uma capacidade de interceptação adequadas sobre a área de interesse (AoI — *area of interest*). O foco principal é a tentativa de encontrar a melhor combinação de sensores, plataformas e pessoal, suas localizações e modos de operação, tendo em atenção a minimização de dois critérios principais: custos globais e risco de segurança.

Assim, a avaliação de riscos é uma componente fundamental, pois ajuda os tomadores de decisão a lidar com as incertezas, produzindo informações oportunas e relevantes no contexto de seu ambiente estratégico. Através da avaliação desse risco, torna-se possível aperfeiçoar as decisões sobre a alocação dos recursos disponíveis para o sistema de proteção. Isto possibilita prevenir e evitar atentados, bem como mitigar eventuais consequências adversas, com maior eficácia em termos de custo, contribuindo assim para uma provisão de uma proteção contra essas ameaças, compatível e adequada.

Podemos afirmar que no âmbito do risco de segurança, as ameaças são análogas à doença na medicina. Os doentes são o alvo da doença e um regime de drogas, cirurgia, alterações do estilo de vida, entre outras medidas ditadas pela ciência, traduz a estratégia de mitigação de risco. Da mesma forma, características específicas do ambiente podem contribuir para o sucesso ou insucesso de um **ataque a instalações portuárias vindo do mar**. Associar estas características a cada componente do risco é o cerne do nosso modelo de risco.

1.2 OBJETIVOS DA TESE

Esta tese possui dois objetivos: o primeiro consiste em propor uma nova metodologia para a avaliação do risco de segurança no espaço para proteção de instalações portuárias perante **ameaças terroristas provenientes do mar**, seja à superfície, seja abaixo da linha de água. Essa avaliação de riscos possui como objetivo produzir informações oportunas para o processo decisório de planeamento de recursos de proteção que devam ser alocados.

Muitas metodologias têm sido desenvolvidas e aplicadas para apoiar decisões de planeamento para proteção de infraestruturas consideradas críticas perante ameaças terroristas. A maior parte dessas contribuições está relacionada com a avaliação probabilística do risco — extensivamente aplicada num contexto de *safety risk* e que também se tornou uma abordagem padrão para apoiar decisões estratégicas relacionadas com *security risk* —; ou com modelos de teoria de jogos, que levam em consideração as potenciais atitudes e inteligência dos agentes terroristas para a definição dos recursos de defesa. Ambas as abordagens são limitadas por aquilo que é viável ou razoável para incluir num modelo matemático, seja por falta de dados ou por causa da dificuldade em estimar um grande número de possíveis estados de natureza ou de possíveis vias de ação para os atacantes e defensores.

Sob o nosso ponto de vista, cada visão para tratar esse problema contribui para um conceito-chave que achamos fundamental: as decisões para alocação de recursos de defesa de um porto devem ser geradas e avaliadas o mais objetivamente possível, apoiadas no conhecimento e julgamento dos agentes de decisão envolvidos. Um sistema de apoio à decisão pode produzir soluções estratégicas de custo-benefício razoável e recomendações para a proteção, apoiado por uma forma mais confiável de avaliação do risco de segurança. Ressaltamos que não pretendemos estimar a probabilidade de ocorrência de uma ameaça terrorista num dado intervalo de tempo, mas antes reconhecer se tal ameaça terá maior ou menor dificuldade em alcançar os seus objetivos. Num contexto marítimo, isto pode ser feito com a adaptação de uma técnica empregue no âmbito militar denominada Avaliação Operacional (AO) (Estado-Maior da Armada, 2004; Wagner *et al*., 1999; Giadrosich, 1995). A principal utilidade da AO é reduzir o risco de um equipamento/sistema não satisfazer a expectativa do utilizador, considerando custo, aspetos cognitivos, doutrina, táticas, vulnerabilidades e tipos de ameaças. A técnica pode ser resumida como um conjunto de procedimentos necessários para o fornecimento de subsídios e elementos de informação, qualitativos e/ou quantitativos, que possam auxiliar no processo de tomada de

decisão baseada nos conceitos de Aspetos Críticos e de Elementos Essenciais de Análise. Os Aspetos Críticos consistem na definição do tipo de ameaça, na definição da área de interesse, do ambiente de operação e nas condições ambientais que registem uma maior possibilidade de ocorrência que possam facilitar ou não as intenções de uma ameaça. Os Elementos Essenciais de Análise correspondem às grandezas que se pretendem estimar ou conhecer e na forma como estas serão recolhidas. Neste trabalho, eles são constituídos por um conjunto de índices de risco estimados num reticulado de pontos da área de interesse baseados nos conceitos de Criticidade, Suscetibilidade e Ineficácia.

A multidisciplinaridade que deriva do alargado número de autoridades envolvidas na administração de um porto leva-nos a um problema de decisão em grupo. É esperado que processos de julgamento em grupo sejam melhores do que os individuais. Todavia, a tomada de decisões, mesmo que seja de um grupo, num contexto de incertezas pode produzir diferentes respostas dependendo da forma como o processo de decisão é conduzido e da capacidade limitada das pessoas processarem informações de maneira objetiva.

Devido a esta característica particular do problema tratado, considerámos a oportunidade de propor um novo método de elicitação de opiniões de um grupo de decisores. A proposta permite alcançar um relativo consenso das opiniões do grupo, levando em consideração as incertezas e problemas de comportamento inerentes a qualquer processo de decisão. Além dessa proposta, observamos durante a investigação do tema abordado a possibilidade de elaborar um método para agregação de funções de utilidade individuais de um grupo baseado na média geométrica dos parâmetros de aversão ao risco.

1.3 ORGANIZAÇÃO DA TESE

Esta tese está estruturada em três partes. A primeira parte compreende este capítulo e o Capítulo 2, onde é feita uma revisão dos diversos conceitos e expressões relacionados com qualquer investigação sobre avaliação de riscos, além de uma síntese das metodologias e de sistemas de apoio à decisão utilizados em avaliações do risco de segurança contra ameaças terroristas.

A segunda é formada pelos capítulos 3 e 4. No Capítulo 3 é apresentado o modelo proposto para a elicitação das opiniões de um grupo de decisores. O capítulo discute o conceito de elicitação e apresenta uma completa descrição da abordagem não paramétrica

de estimação de densidades utilizada no modelo. Tendo em vista o carácter ambíguo e vago das variáveis envolvidas e a propensão de serem avaliadas com base na experiência dos decisores/especialistas ou, até mesmo, por perceção, a abordagem adotada para o problema desvia-se das convencionais, que são baseadas em modos de raciocínio clássico, para apoiar-se em outra, baseada em modos de raciocínio aproximado. O Capítulo 4 faz um enquadramento das regras de decisão sob risco e incerteza estrita, com ênfase na Teoria da Utilidade e sua abordagem multiatributo, além de apresentar um modelo de agregação das curvas de funções de utilidade num contexto com múltiplos decisores com aversão ao risco constante.

A terceira parte é composta pelos capítulos 5 e 6. No Capítulo 5 é apresentada a metodologia proposta para avaliação de riscos perante ameaças provenientes do mar chamada Avaliação do Risco de Segurança Espacial (*Spatial security risk*, SSR). A metodologia está baseada nos conceitos de Criticidade, Suscetibilidade e Ineficácia, que são ajustados a uma escala de medição comum por curvas de utilidade que representam as atitudes dos decisores perante o risco e pelas opiniões elicitadas de acordo com os modelos propostos nos Capítulos 3 e 4.

O trabalho é finalizado no Capítulo 6, com um resumo do que foi exposto, destacando-se as principais conclusões, e com a apresentação de sugestões para trabalhos futuros.

2 RISCO DE SEGURANÇA

2.1 CONSIDERAÇÕES INICIAIS

O estudo do risco sob qualquer contexto é um trabalho complexo, dado que a própria definição da palavra risco não é um conceito unânime. Portanto, acreditamos que há uma série de questões que precisam de ser esclarecidas com o objetivo de propiciar um bom entendimento do problema aqui discutido. Este capítulo visa fazer um enquadramento dos diversos termos e definições disponibilizados na literatura sobre o estudo do risco, nomeadamente no contexto de ameaças terroristas, e está organizado da seguinte forma: na Secção 2.2 faz-se uma explicação acerca do significado da palavra 'risco' e das definições relacionadas; a Secção 2.3 apresenta uma breve discussão sobre incerteza, conceito muitas vezes interpretado como sinónimo de risco e os principais conceitos de uma avaliação de riscos utilizados num processo decisório são apresentados na Secção 2.4.

2.2 RISCO E DEFINIÇÕES

Estudos etimológicos sugerem que a palavra é derivada do latim *risicare*, cujo significado é ousar. Nesta aceção, pode ser entendido como uma escolha, não como uma fatalidade, uma sina ou um destino. No entanto, outra vertente afirma que a palavra vem do grego *rhizikon,* sendo derivada de *rhiza,* que significa "raiz, pedra, corte de terra firme" e era uma metáfora para descrever geografias "cortantes" relacionadas com as viagens marítimas, como rochas submersas que podiam "cortar os navios", ou seja, algo a se evitar no mar.

Risco é um conceito intuitivo e omnipresente na sociedade moderna. Ao se perguntar a diferentes pessoas o que significa, diferentes respostas serão obtidas em função de diferentes contextos. Os significados mais comuns são citados por Slovic e Weber (2002): aqueles que descrevem risco como um perigo, uma probabilidade, uma consequência ou uma ameaça/adversidade em potencial. Pode ser encarado como um conceito nómada aplicado a conteúdos diversos em diferentes campos de saber: economia, medicina, ciência política, engenharia, etc.

Consequentemente, a literatura apresenta diferentes definições para risco. A *Society for Risk Analysis* define risco como o potencial para a ocorrência de eventos indesejados e consequências adversas para a vida humana, a saúde, a propriedade ou o ambiente. Segundo Mun (2004), risco é qualquer incerteza que afeta um sistema de uma forma desconhecida, pelo que as ramificações também são desconhecidas. Aven (2009a) define risco pela combinação de duas dimensões: *(i)* eventos e consequências desses eventos, e *(ii)* as incertezas associadas. Para Kaplan e Garrick (1981), risco é um processo analítico baseado nas respostas a três questões: O que pode acontecer de errado? Qual é a probabilidade de alguma coisa com sérias consequências acontecer? E quais são as consequências expectáveis se alguma coisa de errado acontecer? A partir desta última pergunta formulada por Kaplan e Garrick, risco também é definido como a probabilidade de um evento não desejado ocorrer. Neste sentido, um evento não desejado é caracterizado pelas consequências que vão além de um limite que um decisor pode tolerar ou considerar aceitável. Logo, risco é então definido pela probabilidade de um evento em que as consequências excedem um máximo valor aceitável (Reifel, 2006).

Não existe uma definição universalmente aceite para risco e outras definições podem ser apresentadas. Contudo, todas teriam em comum que risco é alguma coisa relacionada com um possível evento futuro que envolve incertezas sobre consequentes perdas ou danos (Teixeira e Rodrigues, 2012).

A utilização generalizada, embora de forma muitas vezes ambígua, da palavra **risco** conduz ao aparecimento de dúvidas relacionadas com os diversos conceitos e que vão além da definição propriamente dita da palavra. Um destes conceitos, que é assunto deste trabalho, é o de **risco de segurança**. A nomenclatura científica internacional interpreta tal conceito sob dois pontos de vista: *safety risk* e *security risk*. O que distingue um conceito do outro, mas também reforça as suas características de ambiguidade, é justamente a natureza da causa das falhas que podem sobrevir. Quer dizer, se a ocorrência tem como causa um evento (ameaça) acidental, estamos diante de um problema de *safety*,

mas se a causa é um evento (ou ameaça) intencional, defrontamo-nos com um problema de *security*. Assim, *safety risk* está relacionado com um evento acidental, que tanto pode ser físico (produzindo um erro físico-estrutural em algum componente – então visto como um sistema) quanto de concepção (caracterizado por imperfeições na estrutura operacional ou na arquitetura do sistema, tanto na fase inicial de produção quanto nas modificações posteriores). Entretanto, podem ocorrer falhas no sistema derivadas de eventos externos, capazes de produzir erros de interação homem-máquina ou erros de entrada de dados ou informações para o sistema. Mesmo nestes casos, a natureza dos eventos é tipicamente acidental.

Pelo contrário, em *security risk* a intenção humana aparece como o elemento constituinte central do evento, cuja concretização se dá pelo aproveitamento de vulnerabilidades ou deficiências da estrutura física ou operacional do sistema, bem como das suas interfaces com o ambiente em que opera. Erros de interação homem-máquina ou erros de entrada de dados ou informações no sistema podem também resultar de atos de interferência maliciosa, com a intenção humana aproveitando-se de eventuais vulnerabilidades de segurança do sistema. Logo, uma avaliação de riscos sob este enfoque altera a primeira questão formulada por Kaplan e Garrick para "como alguém pode fazer alguma coisa de errado acontecer…". Concluimos, assim, que *security* tem por finalidade, em princípio, assegurar a integridade física e operacional das infraestruturas críticas contra ameaças intencionais. Isto é geralmente feito mediante a implementação de medidas preventivas e de contingência contra tais ameaças. Entretanto, para o estabelecimento dessas medidas, uma infraestrutura crítica deve ser analisada de uma forma tal que as suas principais componentes ambientais e/ou físicas, bem como as suas interfaces, possam incluir atributos correlacionados com os riscos de segurança a que estamos sujeitos. Esta discussão remete para outras palavras que são fundamentais para o perfeito entendimento do conceito de *security risk*: ameaça, vulnerabilidade e infraestruturas críticas.

A definição de ameaça inicia-se pela análise de um fator importante e condicionante que é a motivação. Teorias comportamentais clássicas da psicologia social defendem a tese de que o ser humano só age motivado (Maslow, 1970; Vroom, 1964). Segundo essas teorias, motivação é o processo responsável pela intensidade, direção e persistência dos esforços de uma pessoa para a concretização de uma intenção. Vroom (1964), em particular, acredita que a motivação é o processo que governa ou condiciona a escolha de comportamentos intencionais alternativos. Pode-se admitir, portanto, que a qualquer ato intencional está associada uma motivação. Garrick *et al.* (2004), define

ameaça como uma indicação de algo iminente, ou uma expressão de intenção de infligir o mal, ferimentos ou danos. Definição próxima é a apresentada por Cox (2009b); para este autor, ameaça é qualquer indicação, circunstância ou evento com o potencial de causar perdas ou danos a um ativo ou a uma população. O Departamento de Segurança Interna dos EUA afirma que as ameaças são dirigidas a um alvo enquanto o perigo não, hipótese confirmada por Myagmar *et al.* (2005). Saliente-se que perigos e ameaças são distinguidos principalmente pela motivação, todavia, um perigo pode ser explorado por uma ameaça para concretizar os seus intentos (Garrick *et al*., 2004). Outras definições dizem respeito ao dano ambiental — embora aparentemente feito pelo homem, ou seja, motivado, nem sempre é possível atribuir-lhe uma motivação ou alvo específico. Portanto, a fim de evitar qualquer confusão no entendimento deste conceito usaremos uma definição para ameaça no contexto da avaliação de riscos de segurança que considera os terroristas como agentes motivados e que é adaptada de Garrick *et al*. (2004):

"Ameaça é a intenção de um terrorista infligir dano ou prejuízo a um bem ou um alvo específico, por um específico meio, motivada por interesses ou objetivos ideológicos, políticos ou religiosos."

A manifestação dos estados inerentes do sistema — como por exemplo, físicos, técnicos, organizacionais e culturais — que podem estar sujeitos a um perigo natural ou explorados por uma ameaça que podem causar danos a esse sistema é definida como vulnerabilidade (Haimes, 2009). No entanto, Aven (2007) defende que vulnerabilidade é meramente uma parte de um conceito mais amplo de risco. O mesmo autor afirma que vulnerabilidade resulta da combinação de possíveis consequências e incertezas em função de uma fonte.

A vulnerabilidade pode ser analisada em função de uma cadeia de causas ou fatores, entre eles, naturais, tecnológicos ou políticos. McGill *et al.* (2007) afirmam que um sistema é dito vulnerável a certo grau de perdas ou danos após a ocorrência de um evento específico se existe potencial para, pelo menos, um conjunto de estados do sistema formar um elo entre tais eventos e as consequências indesejadas. Num contexto um pouco diferente, a vulnerabilidade foi brevemente definida por McCarthy *et al*. (2001) como "… o grau de um sistema ser **suscetível** a, ou incapaz de lidar com, efeitos adversos". A partir desta interpretação, Rodrigues (2012) assinala que num contexto de risco de segurança, vulnerabilidade pode ser decomposta em duas partes: suscetibilidade e ineficácia. Ineficácia é a probabilidade de fracasso do sistema de defesa para lidar com uma tentativa de ataque e suscetibilidade é o nível de exposição natural a potencial ataques, não levando

em consideração o sistema de proteção instalado. Estas interessantes interpretações da definição de vulnerabilidade são especialmente úteis quando desejamos fazer uma avaliação do risco de segurança.

O conceito de suscetibilidade no contexto de avaliação de riscos possui várias interpretações que apresentam tendências diferentes tanto em contextos científicos e políticos, como dentro de disciplinas e profissões. As definições incorporam diferentes conceitos que terão maiores ou menores relevâncias concernentes à forma como a suscetibilidade é conduzida no contexto da especificidade da avaliação do risco (Parkin e Balbus, 2000).

Parkin e Balbus (2000) apresentam uma análise das diferentes definições provenientes de diversos campos da ciência, como biologia, ecologia, engenharia, medicina, epidemiologia e toxicologia. Definições relacionadas com o contexto de *security risk* são apresentadas por Richards (2009) e McGill *et al.* (2007). O primeiro autor define suscetibilidade como o grau em que um sistema de armas está aberto a um ataque devido a uma ou mais fraquezas inerentes, definição proveniente do Departamento de Defesa dos Estados Unidos (US-DoD, 2002). Sendo assim, suscetibilidade é considerada como o termo mais preciso para descrever pontos fracos que podem ou não ter o potencial de serem explorados. Os segundos autores não definem explicitamente um conceito específico para suscetibilidade. Porém, usam como sinónimo fatores que podem ser explorados por agentes maliciosos e que possibilitam a identificação de cenários plausíveis, sem a necessidade de recorrer aos dados de inteligência politico-militar, que tentam revelar as intenções do adversário. Assim, podemos concluir que as duas abordagens possuem expressões diferentes, porém, com o mesmo significado: fraquezas inerentes ao sistema, mencionadas pelo primeiro autor, podem ter a mesma interpretação de fatores que podem ser explorados por agentes maliciosos, citados pelos segundos autores.

Verde e Zêzere (2007), num contexto de *safety risk*, definem suscetibilidade como a propensão de uma dada área ou unidade territorial para ser afetada pelo fenómeno estudado, avaliada a partir das propriedades que lhe são intrínsecas. Representa a propensão para uma área ser afetada por um determinado perigo, em tempo indeterminado, sendo avaliada através dos fatores de predisposição para a ocorrência dos processos ou ações, não contemplando o seu período de retorno ou a probabilidade de ocorrência.

As diferentes definições revelam diferentes perspetivas em função do campo de pesquisa onde se deseja avaliar riscos. Este trabalho não tem por objetivo discutir os pontos fortes e fracos das definições disponíveis na literatura e não pretende fazer uma

proposta de uniformização da definição. Porém, seguimos a recomendação apresentada por Parkin e Balbus (2000): num processo de avaliação de riscos a suscetibilidade não deve ser abordada sem a declaração explícita do seu significado, o qual deve estar claramente relacionado com a especificidade da avaliação que se deseja fazer.

Sendo assim, ampliamos o conceito de suscetibilidade apresentado por Rodrigues (2012) devido, principalmente, às características únicas do ambiente onde se pretende fazer a avaliação do risco de segurança investigado neste trabalho. Assim, definimos suscetibilidade como o nível de exposição natural a potenciais ataques, não levando em consideração o sistema de proteção. Representa a propensão de uma área ser explorada por uma *determinada ameaça para alcançar os seus objetivos*, em tempo indeterminado, sendo avaliada através dos fatores de predisposição para a ocorrência dos processos ou ações, não contemplando o seu período de retorno ou a probabilidade de ocorrência.

Criticidade é outro conceito frequentemente encontrado em investigações sobre o impacto ou sobre as consequências esperadas no contexto de avaliação de riscos. O Exército dos Estados Unidos define-o como o grau de importância de uma instalação/equipamento para o cumprimento de uma determinada missão (Trainor, 2007), enquanto Al Mannai (2008), define criticidade como uma medida que descreve o impacto negativo provocado devido à remoção de um ativo pertencente a uma rede de ativos. Outras definições poderiam ser apresentadas, contudo, podemos afirmar que o conceito é tipicamente definido como uma medida das consequências associadas com a perda ou degradação de um ativo. Quanto maior for a ameaça da perda de um ativo, a sobrevivência ou a viabilidade de seus proprietários, ou de outras pessoas que dependam dele, mais crítico este ativo se torna.

Esta secção encerra-se com a apresentação do conceito de infraestruturas críticas, conceito que sofreu diversas adaptações com o decorrer do tempo. Inicialmente, foi definido como sistemas e bens ativos, sejam físicos ou virtuais, que caso fiquem indisponíveis ou destruídos, o impacto sobre a segurança social, a economia, a saúde e a segurança nacional seria preocupante. Posteriormente, essa definição é ampliada para sistemas físicos e cibernéticos essenciais para as operações mínimas da economia e do governo. Esses sistemas incluem, mas não estão limitados às telecomunicações, energia, finanças, transportes, sistemas de água e serviços de emergência, tanto governamentais como privados. Por fim, esta relação de bens e ativos passou a listar monumentos nacionais, estabelecimentos comerciais e serviços governamentais (Lewis, 2006).

2.3 INCERTEZA

A incerteza existe na maior parte dos elementos de uma avaliação de riscos. Riscos envolvem incertezas o que muitas vezes leva a comunidade científica a discutir se são conceitos complementares ou sinónimos. Alguns autores estabelecem que risco é a incerteza sobre o futuro e, consequentemente, risco é igual a incerteza; outros defendem que risco e incerteza são conceitos diferentes que não são independentes um do outro. Adotando esta premissa, podemos afirmar que a incerteza no contexto da avaliação de riscos está relacionada com o grau de confiança que temos nos resultados da análise de riscos. A incerteza depende da qualidade, quantidade e relevância dos dados, além da confiabilidade e da relevância dos modelos e premissas adotados.

Tipicamente, a incerteza é classificada em duas categorias: incerteza aleatória e incerteza epistémica. A incerteza aleatória descreve a variação associada ao sistema físico ou ambiente em consideração, em que esta variação é causada, normalmente pela natureza aleatória dos dados associados ao problema. Exemplos desta categoria são as variações na velocidade do vento, precipitação da chuva, variação das correntes de maré. Enquanto a incerteza epistémica está associada a certo nível de ignorância, ou informação incompleta, do sistema ou ambiente que o rodeia. A incerteza epistémica é usada para descrever qualquer falta de conhecimento ou informação numa fase ou atividade do processo de modelação do sistema. Frequentemente, está presente em situações onde o tomador de decisão solicita a opinião de diversos especialistas, devido à falta de conhecimento suficiente sobre o problema. Por exemplo, para avaliar o impacto de um ataque terrorista a um específico ponto crítico de um porto em função da tática e armamento que possam vir a ser utilizados.

Considerando que a incerteza aleatória é inerentemente irredutível, a incerteza epistémica pode ser reduzida com a aquisição de conhecimentos. As incertezas aleatórias podem ser tratadas por métodos clássicos frequentistas, incertezas epistemológicas só podem ser resolvidas através de métodos bayesianos e/ou opiniões de especialistas. Paté-Cornell (1996) define seis níveis de complexidade na caracterização do risco que leva em conta as incertezas epistémicas e aleatórias em diferentes graus de detalhe:

O **Nível 0** de análise consiste na identificação de um evento indesejado, que é basicamente a identificação de uma potencial ameaça ou na identificação das diferentes formas em que um sistema pode falhar. Por exemplo, um evento indesejado pode incluir

um evento nuclear num porto ou um dispositivo explosivo improvisado (IED) transportado por um mergulhador em uma zona de atracação de navios.

O **Nível 1** de análise é baseado na abordagem do pior caso. Está relacionado com o nível anterior e não envolve qualquer noção de probabilidade, tenta produzir o máximo nível de perda, portanto, só é aplicável quando este nível de perda, limite superior dos resultados, é conhecido.

O **Nível 2** de análise envolve a definição de valores plausíveis para cada cenário onde não são conhecidos claramente os limites superiores dos resultados dos piores casos. Esta análise representa uma tentativa de se fazer uma avaliação das piores condições possíveis que podem ser razoavelmente esperadas quando existe alguma incerteza dos resultados ou quando o pior caso é tão improvável que pode ser desconsiderado, e ser substituído por uma análise de **quase pior caso**. O desafio neste nível de análise é que a definição do limite superior de resultados pode incorporar uma componente subjetiva. O termo "plausível" pode significar algo diferente com base na forma como está sendo usado. A perda máxima plausível de vida como resultado de uma explosão nuclear para uma pequena cidade provavelmente irá variar significativamente em relação a uma cidade maior. Assim, durante a análise deste nível estas incertezas devem ser reduzidas.

O **Nível 3** tem como objetivo produzir uma análise de **melhor estimativa** ou de valores baseados em medidas de tendência central das distribuições de probabilidade dos resultados esperados: a média, a moda ou a mediana. Logo, a definição da função de distribuição é um elemento importante deste nível. A distribuição pode ser definida de forma a apresentar uma maior concentração de resultados no centro da função, mas que ainda leve em conta a dispersão e o comportamento nas caudas.

O **Nível 4** consiste numa análise probabilística do risco. Adiantamos que pode ser definido de forma simples como a obtenção de uma distribuição de probabilidade dos diferentes estados do sistema baseada nas melhores estimativas dos modelos e dos valores dos parâmetros, ou seja, é construída uma curva de riscos. Nesta forma, envolve somente incertezas aleatórias. Este processo será descrito com maiores detalhes na próxima secção.

O **Nível 5** de análise proporciona a exibição das incertezas sobre as hipóteses fundamentais através de uma família de curvas. Isto envolve o uso de análise Bayesiana dos elementos existentes ou o uso da opinião de especialistas sobre os parâmetros de entrada que constituem o modelo de avaliação de riscos. Neste nível, as incertezas epistémicas são representadas por distribuições de probabilidade dos modelos e das hipóteses utilizadas. Para cada uma, os efeitos da aleatoriedade nos resultados são

representados por probabilidades condicionais, e os resultados globais são obtidos através da combinação das medidas de incertezas epistémicas e incertezas aleatórias. Ao contrário do Nível 4, as incertezas devem ser mantidas separadamente na análise, e o resultado é uma família de curvas de risco. Isso representa a principal diferença a partir de um modelo determinista, que utiliza um único valor, por oposição a uma distribuição de valores.

Infelizmente, dada a natureza dos diversos cenários resultantes de um ataque terrorista, torna-se inviável fazer medições reais. Uma melhor abordagem é representar estas incertezas utilizando quantidades que possam ser conhecidas, combinadas com a experiência de especialistas, para as variáveis de decisão (Paté-Cornell, 2002).

2.4 ANÁLISE E AVALIAÇÃO DE RISCO DE SEGURANÇA

Tipicamente, análise de risco de segurança é definida como o uso sistemático das informações disponíveis para a identificação das ameaças e perigos com a finalidade de identificar os riscos para os indivíduos, as propriedades e o ambiente. A análise inclui a identificação das **ameaças**, das **vulnerabilidades** e das **consequências** do impacto (Masse, 2007). A interação dessas três componentes em cenários possíveis, onde os valores a eles atribuídos podem ser agregados entre si, produz uma perceção, permitindo a mensuração dos valores do risco. Esses valores tornam possíveis a ordenação dos riscos e o estabelecimento de prioridades para aplicação de contramedidas de segurança. Os resultados dessa análise são então **avaliados**. Neste momento, cabe ressaltar que a nomenclatura científica internacional regista duas expressões em inglês, ***risk evaluation*** e ***risk assessment***, que são tratadas muitas vezes como sinónimas e possuem a mesma tradução para a língua portuguesa, **avaliação de riscos**. Estes termos estão presentes, inclusive, na definição para avaliação de riscos da norma ISO 31000:2009 (Leitch, 2010):

"***Risk assessment**: overall process of risk analysis and risk evaluation."*

Risk evaluation é um processo que visa definir o que o risco estimado realmente significa para as pessoas interessadas ou afetadas, ou seja, pelos *stakeholders*. Uma grande parte desta avaliação será a consideração de como as pessoas percebem os riscos, levando em consideração aspetos socioeconómicos e ambientais, por exemplo. Conclui-se que, ao se fazer processos de análise de risco e *risk evaluation* de forma conjunta, podemos dizer que estamos perante um processo de *risk assessment* (Fig. 2.1).

Figura 2.1 - Definição de avaliação de riscos

Apesar de não fazer parte da proposta aqui apresentada, achamos necessário apresentar outro conceito que muitas vezes suscita dúvidas e é usado como sinónimo de análise ou avaliação de riscos que é o de gestão de riscos. Gestão de risco é um processo contínuo com o objetivo de definir o conjunto de medidas e atividades produzidas para reduzir ou eliminar danos às pessoas, ao ambiente ou a outros ativos inerentes à exploração de oportunidades (Aven, 2009a). Assim, a gestão do risco é um processo subsequente à avaliação dos riscos onde é possível tentar otimizar as decisões sobre a alocação dos recursos disponíveis para a segurança (tais como equipamentos de inspeção, pessoal treinado, sistemas de vigilância etc.), prioritizando o emprego destes recursos na proteção dos ativos avaliados como mais sujeitos a eventos indesejáveis e ao impacto das consequências negativas dos mesmos. Ou seja, a gestão de risco procura, através de um processo de monitorização e controlo, reduzir tais riscos — e, se possível, virtualmente eliminá-los —, tendo também em consideração os custos associados. A Figura 2.2 ilustra este conceito.

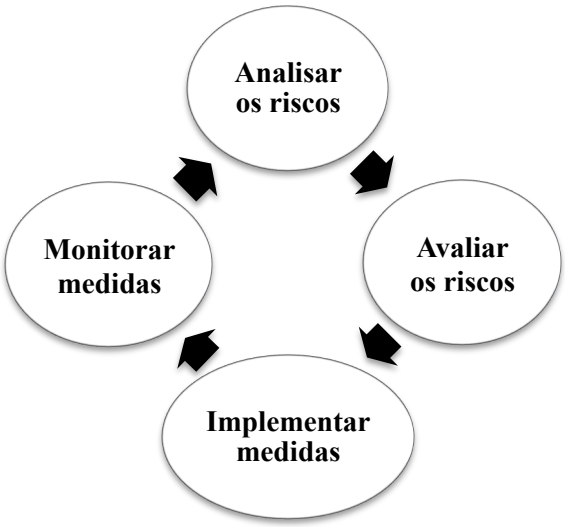


Figura 2.2 - Gestão do risco

2.5 METODOLOGIAS DE AVALIAÇÃO DO RISCO DE SEGURANÇA

Proteger infraestruturas complexas contra terroristas, que são considerados adversários inteligentes, é fundamentalmente diferente de proteger contra acidentes aleatórios ou atos da natureza. As avaliações do risco de segurança têm utilizado metodologias híbridas que associam uma análise qualitativa a uma análise quantitativa na identificação e caracterização do perfil de agressores ou terroristas. Técnicas quantitativas que envolvem análises probabilísticas condicionais de eventos e consequências têm sido desenvolvidas com base na opinião de especialistas, determinando probabilidades subjetivas de ocorrência dos eventos e avaliação conceitual da criticidade dos alvos potenciais, bem como das consequências dos ataques destas ameaças (Willis, 2007).

Um dos métodos mais comuns na condução da avaliação do risco de segurança são as matrizes de risco, que são usadas em diversos contextos, entre eles: risco de terrorismo, gestão de riscos em face de mudanças climatéricas, gestão de projetos, entre outros. Nessas matrizes, podem ser extraídos cenários de risco, de conformidade com as combinações de 2 ou 3 dimensões — por exemplo, frequência e consequência, ou ameaça, vulnerabilidade e consequência. Tais cenários podem ser distinguidos pelas diferentes cores das células da matriz, conforme exemplo da Tabela 2.1. O cenário verde é o de risco mais baixo, enquanto o castanho é o de mais alto risco; as demais cores são riscos intermédios.

Tabela 2.1 - Matriz de riscos

	Consequências				
	Insignificante	**Baixo**	**Moderado**	**Alto**	**Catastrófico**
Quase certo	Significante	Alto	Alto	Extremo	Extremo
Provável	Médio	Significante	Alto	Alto	Extremo
Possível	Médio	Médio	Significante	Alto	Alto
Improvável	Baixo	Médio	Médio	Significante	Alto
Raro	Baixo	Baixo	Médio	Médio	Significante

No entanto, vários estudos indicam que o uso de matrizes de risco pode gerar inconsistências, entre as quais (Cox, 2008):

- Elas podem atribuir idênticas classificações a riscos quantitativamente muito diferentes;
- Podem, equivocamente, atribuir classificações qualitativas mais elevadas a riscos quantitativamente menores;
- Entradas e saídas ambíguas: as entradas para as matrizes de risco (por exemplo, frequência e gravidade) e as saídas resultantes (ou seja, as classificações de risco) exigem interpretações subjetivas e diferentes utilizadores podem obter classificações opostas dos mesmos riscos quantitativos;
- Podem originar alocações de recursos subótimas.

As limitações sugerem que as matrizes de risco devem ser utilizadas com cautela. No entanto, a utilização de matrizes de risco é muito difundida (e conveniente) para avaliar um conjunto de opções. Maiores pesquisas são necessárias para melhor caracterizar as condições sob as quais elas serão úteis ou prejudiciais para avaliar o risco num processo de tomada de decisões.

Diversas abordagens são baseadas em modelos de Teoria dos Jogos, sobretudo a avaliação do risco de segurança para ameaças terroristas. Várias análises teóricas de jogos têm mostrado que os terroristas mudam a sua atenção para alvos mais fáceis e menos complicados logisticamente em reação aos investimentos em segurança feitos pelos defensores (Bier, 2007; Cox, 2009a; Paté-Cornell *et al*., 2002, Brown *et al*., 2011). Esse tipo de abordagem considera explicitamente a modelação das preferências e ações dos terroristas, e requer também probabilidades difíceis de estimar. Modelos suficientemente realistas podem ser difíceis de optimizar, devido ao elevado número de estados possíveis quer para os meios de defesa, quer para as ameaças, quer para as condições ambientais. Essa complexidade será bem maior se a análise não se centrar na proteção de uma única infraestrutura, mas sim na proteção de toda uma área portuária.

Um terrorista deve, em geral, ser considerado um agente inteligente, capaz de adaptar as suas estratégias — quando, onde e como atacar — em função das mudanças no ambiente do teatro de operações. Além disso, um terrorista pode ser considerado um agente racional, capaz de conceber estratégias de ataque fundamentadas tão racionalmente quanto o faz a defesa (Ellingsen, 2009). A principal dificuldade não é modelar o problema

como um jogo, de forma analítica, mas sim conseguir que esse exercício seja suficientemente realista — tendo em consideração o elevado número de estados possíveis — e tenha real aplicação prática. Nomeadamente, é necessário saber antecipar suficientemente bem os possíveis comportamentos de um terrorista, mas também estimar as suas escalas de valor. Referimo-nos, em especial, aos conceitos de utilidade e, de certa forma, de aversão ao risco — pelo menos, o receio de falhar um ataque e ser capturado.

A análise opositória, ou adversarial (*adversarial analysis*), é mais fácil de conseguir por via da simulação do que por via analítica. O objetivo não será então obter soluções de defesa ótimas, mas sim avaliar experimentalmente soluções interessantes, procurando encontrar vulnerabilidades não antecipadas inicialmente (Caiti *et al*., 2012; Xu, 2009). Um simulador é, então, tipicamente um instrumento para a realização de exercícios de *red teaming*, em que o comportamento dos atacantes é ensaiado por operadores humanos ou está previamente descrito por *scripts*, segundo o paradigma informático da simulação de agentes inteligentes.

A técnica de análise *Failure Mode and Effect Analysis* (FMEA) foi desenvolvida nos anos 50 por engenheiros de fiabilidade, para identificar problemas que poderiam surgir do mau funcionamento de sistemas militares. FMEA é um procedimento por meio do qual cada modo de falha potencial num sistema é analisado para determinar o seu efeito no sistema e para classificá-lo de acordo com o seu grau de severidade. Quando a FMEA é ampliada por uma análise de criticidade, a técnica é denominada de *Failure Mode and Effects* ***Criticality*** *Analysis* (FMECA). Uma aplicação desta técnica na avaliação do risco de segurança é apresentada por McGill *et al*. (2007). Uma característica desta técnica prende-se com o facto de que a incerteza e a imprecisão são entendidas como derivadas da ambiguidade e da indefinição das variáveis envolvidas e não da falta de conhecimento sobre elas ou da aleatoriedade dos seus valores.

Em muitas pesquisas, a avaliação de riscos envolve o uso de métodos de pontuação. Nestes métodos, características intrinsecamente quantitativas ou qualitativas são expressas por variáveis de escalas ordinais cujos níveis são atribuídos subjetivamente por um avaliador. Um exemplo de aplicação desta abordagem é apresentado por Berbash (2010), baseado no trabalho de Tzannatos (2003), para definir o nível de ameaças terroristas às instalações de um aeroporto e é reproduzido na Tabela 2.2, que descreve em detalhe como são definidos os níveis da ameaça.

Tabela 2.2 - Classificação dos níveis de ameaça (Berbash, 2010)

Level	*Threat description*	*Score*
Very High	*Identifies a credible threat to airport assets, so that continuous or intensive attacks are likely to occur, and that the adversary demonstrates the capability and intention of launching an attack targeting the airport or one of its assets on a frequently occurring basis, and specialized security advice should be sought.*	**5**
High	*Identifies a credible threat to airport assets based on knowledge of the adversary's capability and intention of attacking airport assets that involve high levels of expertise, resources, and support and based on related incidents having taken place at similar airports or in similar situations.*	**4**
Medium	*Identifies a possible threat to airport assets based on the adversary's desire, limited expertise, resources, or opportunity to compromise similar assets.*	**3**
Low	*Identifies random low-level subversion threats to airport assets, with few known adversaries who would pose a threat to airport assets, involving low levels of expertise and resources.*	**2**
Very low	*Identifies an attack is unlikely to occur or that there is credible evidence of capability or intent, with no history of actual or planned threats against airport assets.*	**1**
None	*No threats*	**0**

Hubbard e Evans (2010) identificam alguns problemas nesta abordagem. Em primeiro lugar, não levam em consideração os aspetos psicológicos e vieses cognitivos que interferem na capacidade das pessoas para avaliar riscos. Em segundo lugar, as definições qualitativas que são relacionadas com as escalas ordinais podem ser interpretadas de formas diversas entre os diferentes utilizadores ou até mesmo pelo mesmo utilizador aquando de uma segunda avaliação; desta forma, os resultados podem ser bastante inconsistentes. Em terceiro lugar, muitos utilizadores tratam essas escalas como se elas fossem escalas de razão, resultando em inferências inválidas. Uma escala ordinal classifica as unidades em classes ou categorias quanto à característica que representa, estabelecendo uma relação de ordem entre as unidades pertencentes a categorias distintas, designando uma posição relativa das classes segundo uma direção. Entretanto, uma variável ordinal não possibilita a comparação de diferenças entre unidades com respeito à característica que ela exprime. Nessas circunstâncias, qualquer variável com o mesmo número de valores e com a mesma ordenação desses valores é igualmente apropriada para a expressão da característica. Tais variáveis são geralmente inconvenientes, por exprimirem uma característica contínua de modo muito impreciso. Isso pode levar os utilizadores a fazer inferências inválidas, que podem, por vezes, ser prejudiciais. Por exemplo, a classificação pode originalmente ser avaliada numa escala verbal de cinco pontos e, posteriormente, convertida numa representação numérica para facilitar o processamento, como é o caso da Tabela 2.2. Se a classificação "muito pouco provável" é convertida no valor numérico 2, e "muito provável" é convertida no valor numérico 4, então alguém desprevenido pode inferir que o nível do risco dessa última categoria é exatamente o dobro da primeira. Essa

inferência é falsa, uma vez que as escalas ordinais envolvem uma métrica de distância indeterminada.

Há muitos anos que a análise probabilística do risco (*probabilistic risk analysis*, PRA), também encontrada na literatura sob o nome de avaliação quantitativa do risco, tem sido uma importante ferramenta empregue em diversos contextos de *safety risk*, como impacto ambiental, medicina e projetos da indústria. Consequentemente, modelos de PRA não deixariam de existir para *security risk*.

Têm sido desenvolvidos modelos quantitativos, especialmente, modelos de análise de risco, que envolvem análises probabilísticas condicionais de eventos e respetivas consequências. Nesse contexto, as abordagens mais comuns encontradas na literatura são as abordagens analíticas baseadas na formulação "*TVC*" (Willis, 2007):

$$\text{Risco} = T \times V \times C \qquad \textbf{(2.1)}$$

onde ***T*** representa a probabilidade de ocorrência de uma ameaça, originando um ataque. A componente ***V*** refere-se à vulnerabilidade do sistema, sendo definida como a probabilidade de um ataque ser bem-sucedido caso seja tentado, e a sua minimização representa a melhor, se não mesmo a única, oportunidade para a defesa conseguir reduzir o risco global. Por último, ***C*** representa as consequências de um ataque bem-sucedido. Podemos traduzir esta definição como sendo uma probabilidade (a combinação dos dois primeiros fatores) multiplicada pelas consequências, ou seja, o valor esperado dos danos, caso não seja reduzido o fator de vulnerabilidade.

Essa abordagem é a base para todos os processos de avaliação de riscos usados pelo governo dos Estados Unidos como podemos ver nas citações abaixo:

-"*The cornerstone of the National Infrastructure Protection Plan is its risk analysis and management framework that establishes the processes for combining consequence, vulnerability, and threat information to produce assessments of national or sector risk."* (US-DHS, 2009).

"*In our framework, risk assessment is a function of threat, vulnerability, and consequence. The product of these elements is used to develop scenarios and help inform actions that are best suited to prevent an attack or mitigate vulnerabilities to a terrorist attack, in conjunction with the risk-based evaluation of alternatives undertaken while considering cost and other factors."* (US-GAO, 2005).

Consequentemente, diversos organismos têm adotado sistemas para avaliação de riscos baseados na fórmula $T \times V \times C$, entre os quais podemos citar:

RAMCAP, *Risk Analysis and Management for Critical Asset Protection*. Composto por sete etapas na análise de risco: (1) Definição dos ativos da área a ser protegida; (2) Caracterização das ameaças a partir de dados de sistemas de inteligência; (3) Análise das consequências – medida em custos financeiros, mortes e feridos; (4) Análise de vulnerabilidades – a partir da determinação da probabilidade de um ataque bem-sucedido usando uma ameaça específica contra um determinado ativo; (5) Avaliação da ameaça – com base em avaliações de inteligência do adversário, suas capacidades e intenções; (6) A avaliação de risco – uma avaliação sistemática e abrangente do cenário de ataque terrorista em um determinado ativo. Por último, a gestão de riscos – implementação de ações para atingir um nível aceitável de risco a um custo aceitável.

MSRAM, *Maritime Security Risk Analysis Model*, é uma ferramenta usada pela Guarda Costeira dos EUA (USCG) para analisar o risco de terrorismo. Baseia-se em cenários que combinam tipos de alvos e modos de ataque. A probabilidade de ocorrer um ataque é estimada a partir de informações do serviço de inteligência. A avaliação de vulnerabilidade é feita com base em fatores tais como a dificuldade de ataque, a capacidade da Guarda Costeira interditar um ataque, e a capacidade do alvo para resistir ao ataque. A consequência é definida como o impacto negativo de um ataque bem-sucedido e é medida em termos de lesões/mortes, o impacto económico, o impacto ambiental, os impactos de segurança nacional e impactos simbólicos. MSRAM é uma ferramenta de gestão de ativos que avalia o risco com base nos seguintes elementos: capacidade do terrorista para realizar um ataque bem-sucedido, capacidade da USCG interromper o ataque; capacidade local, estadual e federal para detê-lo; capacidade do proprietário/operador para interditar a ameaça; e capacidade do alvo para resistir a um ataque. A derivação de probabilidades não é especificada. Combinar estes cinco elementos que contribuem para uma única estimativa de probabilidade é certamente um desafio, especialmente, como observado anteriormente, porque diferentes pressupostos poderão ser feitos sobre cada elemento.

TRAM, *Transit Risk Assessment Tool*, é um sistema desenvolvido pelo Departamento de Segurança Nacional do EUA voltado, especificamente, para o setor dos transportes. O processo de avaliação de riscos é idêntico ao do sistema MSRAM e trabalha de forma agregada a este. Os principais objetivos da ferramenta são avaliar os riscos

relativos a atos de terrorismo contra os ativos críticos de propriedade e / ou operados por agências de transporte.

MBRA, *Model-Based Risk Assessment*, é uma ferramenta que utiliza modelos de redes para identificar os ativos mais críticos. O objetivo é avaliar os riscos e definir estratégias de alocação de recursos que reduzam os riscos sobre o sistema. É uma abordagem ao nível do sistema, não uma abordagem a nível de ativos. Portanto, o valor do risco calculado a partir da fórmula *TVC* é toda a infraestrutura, não é apenas de um dos ativos que a compõem.

Apesar de largamente utilizada, a literatura afirma que essa metodologia não é eficiente para modelar o comportamento de atacantes inteligentes e para a alocação de recursos e apontam uma série de limitações em modelos desenvolvidos com esta abordagem. Em particular, a Equação 2.1 assume que a componente ***T*** reflete a probabilidade de um ataque num intervalo de tempo. Para definir esta incerteza aleatória precisaríamos de construir uma população infinita de formas de ataque similares de forma a extrairmos a taxa de sucesso representante da probabilidade de um ataque bem sucedido. Tal não é viável para fenómenos que ocorrem de forma muito esporádica, como é o caso de ataques terroristas (Aven, 2010). Outros autores também afirmam que será sempre muito duvidosa a fiabilidade das estimativas em forma de probabilidades, a partir da opinião de especialistas baseados em dados de inteligência, num problema considerado de profunda incerteza (Aven, 2009b; Brown e Cox, 2011; Cox, 2012). Probabilidades podem ser usadas como uma ferramenta útil para expressar incertezas, todavia, podem provocar interpretações erróneas, porque estão condicionadas a um específico conhecimento que inclui hipóteses e suposições. A razão disso é que a fonte de risco é um adversário inteligente, contra o qual ainda não existe muita experiência. Ao contrário de forças naturais, os adversários têm a liberdade de escolher um modo de ataque e tipo de alvo para chegarem mais perto de cumprir os seus objetivos. Como resultado, as probabilidades e consequências de um ataque terrorista tornam-se difíceis de prever.

Consequentemente, isto levou a comunidade de segurança a aceitar ataques maliciosos como uma nova espécie de problemas (Slovic, 2002), o que coloca o quadro de aceitação de ataques maliciosos como parte do curso normal dos “negócios” (Resnyansky, 2006). Ou seja, a ideia de que um ataque intencional ocorrerá é frequentemente tomada como um dado adquirido (a probabilidade de ataque é igual a 1), a ênfase é dada no problema de analisar se os ataques são **suscetíveis** de ocorrer ou não.

Keeney e Winterfeldt (2010) argumentam que a avaliação das consequências deve ser feita por um modelo de valor multicritério a partir de um conjunto de objetivos fundamentais a partir do ponto de vista dos agentes de decisão. De modo geral, nos problemas relacionados com riscos de segurança, os objetivos fundamentais dos decisores e da população em geral consistem em reduzir os diversos tipos de consequências que podem ocorrer. Tais preocupações, normalmente, incluem em primeiro lugar os aspetos da saúde física e os danos económicos. Porém, num segundo plano, também podem incluir os danos psicológicos, os danos políticos e, também, aspetos indiretos, por exemplo, a forma como o risco é percebido. Portanto, concordamos que análises comparativas do risco de segurança devem ser comparadas com vários critérios que permitam descrever toda essa gama de preocupações.

No entanto, muitos trabalhos estruturam o problema considerando o ponto de vista dos terroristas. Neste contexto, partem do princípio que os terroristas são agentes racionais. Um agente é dito racional se faz o que é certo com os dados que possui. O certo é o que induz ao sucesso (Abrahms, 2008). Citamos os trabalhos desenvolvidos por Rosoff (2009), onde, a partir da opinião de especialistas, é construída uma árvore de valores que procura descrever um conjunto de objetivos hierárquicos de acordo com as crenças defendidas por líderes terroristas; por Bhashyam e Montibeller (2012), que inferem como os objetivos dos terroristas podem mudar ao longo do tempo e como esta análise pode apoiar o processo de avaliação de risco; e por Wang e Bier (2011), que apresentam um modelo da teoria dos jogos para explorar como a incerteza sobre as preferências terroristas afetam a alocação de recursos.

Acreditamos que em processos decisórios em ambientes caracterizados por situações de grandes incertezas é necessário adotar uma perspetiva mais prudente para apoiar o processo de decisão. Sendo assim, nesta tese consideramos as preferências dos agentes de decisão na elaboração dos objetivos fundamentais no contexto do problema, considerando normas já existentes sobre a segurança dos mesmos e a revisão da literatura.

A metodologia Bayesiana tem sido utilizada por alguns analistas na avaliação de probabilidades de um ataque terrorista bem-sucedido contra um alvo específico. Na análise Bayesiana, os analistas avaliam o estado atual do conhecimento relativo ao ataque terrorista em apreço, coligem novos dados e informações para determinar as questões remanescentes e então atualizam e refinam a sua compreensão para incorporar tanto os dados e informações novos quanto os anteriores.

3 INSTRUMENTOS ANALÍTICOS PARA ELICITAÇÃO

3.1 CONSIDERAÇÕES INICIAIS

A metodologia de avaliação de riscos proposta possui, como uma das suas principais características, o facto de tentar reduzir as fortes incertezas envolvidas no planeamento de medidas de proteção contra um ataque terrorista a partir da análise de dados quantitativos objetivos, que são escassos neste tipo de problema. Contudo, faz-se necessário nessa análise ouvirmos as opiniões de especialistas. Além disso, as decisões relacionadas com a proteção de um porto contra quaisquer tipos de ameaças podem ser da responsabilidade de uma única pessoa, ou de um pequeno grupo. Por analogia, podemos afirmar que a decisão é da responsabilidade de um "ditador benevolente" (uma pessoa ou um pequeno grupo), que deseja — no nosso problema é obrigatório —, ter em conta o ponto de vista dos outros (Keeney e Kirkwood, 1975). Portanto, as preferências do grupo precisam ser conhecidas e consideradas, e isto deve ser feito com base no direito ou mesmo na responsabilidade sobre determinado assunto.

Todas essas opiniões e preferências supracitadas podem ser coligidas através de um processo de elicitação (tradução livre para o português da palavra *elicitation*). No tocante às opiniões de especialistas no contexto do nosso problema, estas estão relacionadas, fundamentalmente, com o potencial de danos que podem ser provocados pelos específicos tipos de ameaças e com o nível de dificuldade de se iniciar um ataque pelo mar devido aos fatores ambientais predominantes na área de interesse. Por outro lado, as preferências dos decisores dizem respeito, sobretudo, com: definição do grau de importância dos mapas de risco para ameaças abaixo da água e à superfície; definição dos pesos dos critérios e dos respectivos valores das escalas de avaliação do impacto esperado

de um potencial ataque; e, definição do nível base deste mesmo índice de criticidade (detalhes são apresentados no Cap. 5).

Uma avaliação de riscos com várias partes envolvidas no processo de tomada de decisão pode ser vista como um problema de decisão em grupo. Decisões em grupo costumam ser mais complexas quando comparadas com decisões individuais, uma vez que diversos fatores contraditórios estão envolvidos. Nesta modalidade, em particular, surgem algumas questões decorrentes da participação e interação entre diversas pessoas, tais como: objetivos individuais conflitantes, ou falta de conhecimento e de motivação dos envolvidos. No nosso problema permanece como prerrogativa – e responsabilidade – do decisor, integrar essas considerações. Para que isto aconteça, todos devem trabalhar de forma cooperativa visando uma convergência de posições que possibilite uma situação de consenso. O termo consenso, tradicionalmente, significa um acordo estrito e unânime entre todas as pessoas envolvidas num processo de tomada de decisão. Ness e Hoffman (1998) definem consenso como "... uma decisão que deve ser alcançada, quando a maioria dos membros de uma equipe concorda com uma opção clara e os poucos que se opõem a ela pensam que tiveram oportunidade razoável para influenciar na escolha. Todos os membros da equipe concordam em apoiar a decisão".

Um procedimento que trata esta questão de forma estruturada é o Método Delphi (Linstone e Turoff, 2002). Inicialmente, foi desenvolvido para elicitar a opinião de especialistas, mas na literatura são encontradas diversas aplicações do método, inclusive para elicitar preferências (Goetz *et al*., 2009). O método Delphi visa a formação de um consenso a partir de uma série de questionários enviados a um painel de indivíduos selecionados, com um coordenador forte e mantendo o anonimato dos participantes. Embora seja um comprovado instrumento de pesquisa, a aplicação tradicional do método não está isenta de críticas, porque apesar de se buscar a convergência das opiniões, ele não consegue capturar as incertezas e vieses de comportamento presentes devido à natureza subjetiva de qualquer processo de elicitação.

Um argumento para minimizar esses problemas está voltado para procedimentos que proporcionem o relaxamento de opiniões precisas sobre o problema em questão que são comummente utilizadas em diversos processos de elicitação. Esta posição é defendida na literatura com uma série de estudos sobre as dificuldades das pessoas expressarem valores exatos como tradução dos seus julgamentos conforme o método Delphi tradicional.

Tendo isto em consideração, fazemos uma proposta com o objetivo de minimizar essas deficiências. O nosso procedimento, chamado **método Delphi Intervalar,** segue

todas as etapas do método Delphi tradicional, porém, permite que os agentes de decisão e especialistas envolvidos expressem, respetivamente, as suas preferências (relacionadas com os parâmetros dos modelos de apoio à decisão citados anteriormente) e as suas opiniões através de intervalos de valores. A representação por meio de um intervalo parece ser uma forma mais realista para lidar com problemas relacionados com estimativas de valores desconhecidos, bem como na definição de valores que representem as nossas preferências. Apoiamos esta afirmação no facto de os valores das nossas preferências, normalmente, não serem armazenados com precisão nas nossas mentes. Além disso, a estimativa pontual de variáveis de interesse onde não se conhece o verdadeiro valor, mesmo que sejam utilizados especialistas no assunto em questão, pode tornar-se uma tarefa difícil, simplesmente porque é impossível mensurá-las com precisão.

A nossa proposta, através da estimação de densidades, permite descrever de forma mais natural a incerteza associada a um conjunto de estimativas ou a um conjunto de valores que refletem as nossas preferências. O conhecimento da função densidade de probabilidade da variável em estudo permitirá descrever melhor o comportamento esperado para o futuro do processo em causa, contribuindo decisivamente para o processo de tomada da melhor decisão. No nosso modelo, a função de densidade do grupo é definida por um modelo não paramétrico, a partir do qual podemos fazer inferências. Trata-se de uma abordagem, com ênfase no método do *kernel*, que tanto pode ser usada para a elicitação da opinião de especialistas como para a elicitação de preferências.

O restante deste capítulo inicia-se com uma discussão sobre procedimentos de elicitação, abordando questões sobre a elicitação de preferências e de estimativas, calibração de opiniões e o consenso de um grupo. Na secção seguinte apresentamos o Método Delphi com todas as suas características. Finalmente, nas duas últimas secções, é feita uma completa descrição de uma das contribuições deste trabalho, intitulada Método Delphi Intervalar, e são discutidos 2 estudos de casos.

3.2 ELICITAÇÃO

Elicitação — ou, segundo alguns autores, *eliciação* — é uma palavra encontrada na literatura sob dois aspetos: elicitação de opiniões de especialistas sob a forma de estimativas, e elicitação de preferências de decisores, partes interessadas (*stakeholders*) ou outros agentes de decisão.

Slottje *et al.* (2008) definem elicitação como uma abordagem sistemática com a finalidade de sintetizar julgamentos subjetivos sobre um assunto em que existe incerteza devido à falta de dados ou quando os dados são inatingíveis devido a restrições físicas ou a falta de recursos. Essa elicitação, segundo Wilson (2013), é, normalmente, representada através de probabilidades subjetivas, sendo que uma das formas mais simples é pedir ao especialista que indique a probabilidade de um evento qualquer acontecer. Por exemplo: "Qual é a probabilidade de chover amanhã?". Muitos estudos têm feito perguntas semelhantes a um grande número de especialistas com o intuito de avaliar se eles podem identificar as probabilidades de eventos desconhecidos. Os resultados são normalmente apresentados através de uma "curva de calibração", onde são comparadas as probabilidades subjetivas estimadas e a verdadeira frequência relativa observada. A conclusão obtida é que, normalmente, os especialistas tendem a empurrar as suas opiniões em direção a 0 ou a 1 de forma mais pronunciada do que registado nas frequências reais.

Um especialista pode ser definido como uma pessoa muito hábil, com profundo conhecimento em algum campo especial do conhecimento e a sua opinião é um julgamento formal sobre um assunto em questão ou pode significar uma crença baseada em informações ou conhecimentos incertos. Logo, é uma avaliação subjetiva, uma estimativa da qualidade ou quantidade de algo de interesse, que parece válido, verdadeiro ou provável na mente do especialista (Ayyub, 2001).

A elicitação de preferências possui similaridades com a elicitação das opiniões de especialistas, porém, pode ser mais complexa e definida como um processo cujo objetivo é definir o valor de parâmetros relacionados com modelos de apoio à decisão. Tais parâmetros são tipicamente subjetivos e envolvem algum juízo de valor. Por exemplo: pesos de critérios em modelos de avaliação multicritério e parâmetros de aversão ao risco de acordo com a Teoria da Utilidade. Lichtenstein e Slovic (2006) assinalam que a necessidade de um processo de elicitação de preferências muitas vezes ocorre em situações com as quais os agentes de decisão não estão familiarizados, alguns dos elementos de decisão são desconhecidos e onde há conflitos no tocante às preferências.

O termo preferência é usado em múltiplos contextos. Economistas e outras ciências sociais frequentemente equiparam preferência como uma escolha ou algo que estão dispostos a pagar (Simonson, 2008). No entanto, psicólogos assinalam que preferência é uma tendência a considerar algo desejável ou não desejável. Nesta interpretação, preferências são equivalentes a atitudes e são tipicamente medidas através de escalas de classificação (Zajonc, 1980; Warren *et al*., 2011). A literatura também menciona

que valores e preferências são termos tratados sem distinção – uma preferência por um estado do mundo sobre outro estado significa que o primeiro é mais valorizado que o segundo. Todavia, as preferências também estão sujeitas a vieses, podem ser influenciadas e adaptadas durante o processo de tomada de decisão, especialmente se as consequências atingirem um longo período de tempo — por exemplo, as preferências das pessoas entre diferentes estados de saúde ao longo da vida podem afetar a tomada de decisões públicas sobre alocação de recursos médicos (Torrance, 1986; Kharroubi *et al*, 2013).

Diversas pesquisas e intensos debates em diferentes campos da ciência, como psicologia, estatística e análise de decisão, discutem a forma adequada de tratamento de um processo de elicitação, qualquer que seja o seu propósito. Devido às diferentes características das áreas envolvidas, diferentes problemas são relatados nesse processo. Apesar das diferenças, existe uma concordância no que diz respeito ao facto de a análise não dever ter apenas em conta quais as perguntas que devem ser feitas, mas também a forma como essas perguntas são feitas. Estes factos têm levado esse campo da pesquisa a ser fortemente influenciado pelos aspetos psicológicos e cognitivos, que influenciam a forma como as pessoas representam as suas informações a respeito de variáveis incertas e como elas respondem a essas informações. Inicialmente, estudos foram feitos por Tversky e Kahneman (1974) que identificaram três tipos de heurísticas frequentemente usadas pelas pessoas na definição das suas opiniões: heurísticas da Representatividade, da Disponibilidade e da Ancoragem. Mais recentemente, Gilovich *et al*. (2002) fizeram uma atualização de diversos outros tipos de heurísticas. A investigação tem prosperado em várias frentes e existe uma vasta literatura sobre este tema, em grande parte dedicada a identificar os fatores que a influenciam, como os trabalhos apresentados por Speirs-Bridge *et al.* (2010), Lin e Bier (2008), Tsai *et al.* (2008), Tetlock (2005).

Com isso, protocolos são projetados para eliminar, ou pelo menos minimizar, esses potenciais problemas. Alguns são discutidos por Morgan e Henrion (1992), Cooke e Goossens (2004), Hora (2007) e Naamani-Dery *et al.* (2015). Existem numerosas diferenças entre os protocolos, porque eles são construídos, sobretudo, em função do ambiente em que são empregados. Contudo, a elaboração de qualquer protocolo deve vislumbrar atividades que permitam lidar com diferentes perspetivas, com diferentes disciplinas, interesses conflituosos e restrições de tempo.

Outro ponto importante em protocolos de elicitação está diretamente relacionado com a qualidade da informação gerada. Sempre que possível, devemos procurar conhecer o desempenho dos participantes do processo, especialistas ou agentes de decisão. Este

desempenho pode estar vinculado à experiência no assunto em questão, à posição hierárquica ocupada na organização ou definido através de um processo de calibração.

Diversos profissionais, engenheiros, técnicos, entre outros, não gostariam de usar um instrumento de medição caso não estivesse calibrado. De forma análoga, também devemos aplicar uma medida de algum tipo para avaliar se a participação dos membros do processo está condizente, ou seja, se as suas opiniões e até mesmo as suas preferências são consistentes, em outras palavras, se estão calibrados. Podemos inferir que eles serão inconsistentes caso deem respostas completamente diferentes, mesmo para um cenário idêntico apresentado em momentos diferentes.

Uma das formas de avaliar o desempenho dos julgamentos de especialistas é através de uma regra de pontuação. Formalmente, uma regra de pontuação é uma fórmula que pode ser pensada como uma forma de recompensa. Lin e Bier (2008) afirmam que a ponderação diferencial de especialistas é importante, uma vez que existem diferenças significativas entre eles.

Basicamente, existem três tipos de regras de pontuação:

- Autoavaliação: cada decisor faz uma autoavaliação, na forma de um intervalo de confiança, para cada uma das suas respostas;
- Pontuação coletiva: cada decisor faz uma avaliação dos outros decisores, na forma de intervalos de confiança;
- Medidas de entropia e informação: as pontuações são determinadas de acordo com uma regra de confiabilidade.

Um dos métodos mais sofisticados é o desenvolvido por Cooke (1991), que combina medidas de entropia e informação baseadas no desempenho de especialistas na avaliação de "variáveis-semente". Estas são quantidades cujo verdadeiro valor é conhecido pelo coordenador do processo de elicitação, porém, não é conhecido pelos especialistas.

O processo é ainda mais complexo quando a decisão envolve um grupo de decisores ou de diversos especialistas, pois as preferências e as opiniões podem ser divergentes, e pode haver agendas escondidas. Neste contexto, as opiniões podem ser elicitadas de forma independente e depois combinadas visando um consenso. A literatura apresenta abordagens matemáticas e comportamentais para esse problema. Sob o ponto de vista das abordagens comportamentais, um método simples consiste em proporcionar a possibilidade de discussão conjunta a respeito dos valores quantitativos ou qualitativos a serem elicitados. Esta abordagem requer um coordenador forte, com capacidade para lidar com membros do grupo com personalidades fortes, que tentam impor as suas opiniões, e

que saiba identificar a polarização de respostas entre subconjuntos do grupo e o desejo de harmonia que substitui a interpretação realística do problema por um simples consenso.

Como o problema abordado envolve múltiplos decisores e, provavelmente, diversos especialistas, devido à heterogeneidade do ambiente em que se processa a avaliação de riscos, torna-se conveniente um processo estruturado de interação que providencie um *feedback* aos especialistas e decisores, de forma a facilitar a criação de uma situação de relativo consenso. Sendo assim, considerando as questões expostas, o método Delphi é uma das potenciais técnicas disponíveis que pode servir de base para o processo de elicitação das opiniões e preferências necessárias no nosso problema.

3.3 MÉTODO DELPHI

Segundo Linstone e Turoff (2002), Delphi é um método caracterizado como uma técnica que busca o consenso de um grupo a partir de um processo de comunicação, visando tratar um problema complexo de forma eficiente. Parenté *et al.* (2005) argumentam que o método é uma ferramenta com potencial para a análise de cenários de riscos, bem como para a análise de eventos incertos, tais como: mudanças geopolíticas, ações militares e atividades terroristas. Um exemplo de aplicação do método Delphi neste último contexto é apresentado por Van der Linde e Van der Duin (2011).

O método foi desenvolvido nos anos 50 pela *RAND Corporation*, instituição sem fins lucrativos, com sede na Califórnia, que realiza pesquisas relacionadas com a tomada de decisões e a implementação de políticas nos setores público e privado. Conceitualmente, o método é bastante simples e está baseado no princípio de que a opinião de um grupo é mais válida do que as opiniões individuais. Trata-se de um questionário interativo, que circula repetidas vezes por um grupo, preservando o anonimato das respostas individuais. Cada membro do grupo recebe um questionário, preparado por uma equipa de coordenação, onde lhe são pedidas, usualmente, respostas quantitativas apoiadas por justificações e informações qualitativas. As respostas às questões quantitativas são tabuladas, recebendo um tratamento estatístico simples —definindo-se, normalmente, a mediana e os quartis —, e os resultados são devolvidos aos participantes.

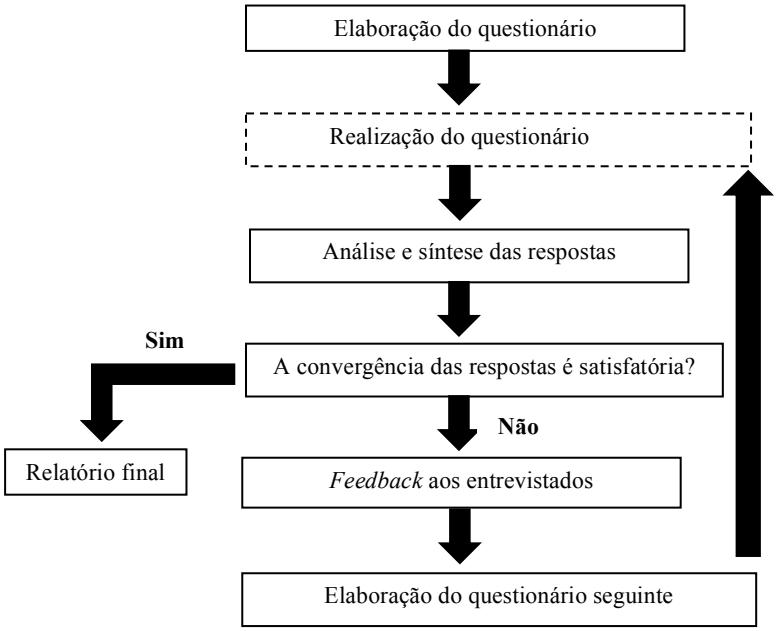


Figura 3.1 - Etapas do método Delphi

A cada nova ronda, a equipa de coordenação deve decidir a respeito da necessidade de incorporar novas questões na ronda seguinte ou simplesmente repetir as perguntas do questionário anterior. Obrigatoriamente, as respostas a um questionário devem ser apresentadas a todos os participantes na ronda de perguntas que se segue. Este procedimento estabelece um *feedback* entre os participantes, pois permite a troca de informações entre eles e, em geral, conduz a uma convergência rumo a uma posição de consenso, sendo esta uma das principais características do método. O processo é repetido até que a divergência entre os participantes seja reduzida a um nível satisfatório e a resposta da última ronda seja considerada como a resposta do grupo. A Figura 3.1 resume o método.

Para a elaboração do questionário de perguntas, o coordenador, ou a equipa de coordenação, do painel Delphi deve procurar informações sobre o tema, recorrendo à literatura ou a especialistas no assunto em questão. Quando se trata de um problema de grande abrangência e complexidade, pode-se recorrer a técnicas de estruturação de problemas – como a análise morfológica, ou outros instrumentos de apoio.

O anonimato das respostas e o facto de não haver uma reunião física reduzem a influência de fatores relacionados com aspetos do comportamento humano, como, por exemplo, a relutância em abandonar posições assumidas e a dominância de grupos maioritários em relação a opiniões minoritárias. Não é, no entanto, a natureza explícita do problema que determina a utilização do método, mas sim, as circunstâncias particulares

associadas em torno do processo de comunicação do grupo. Geralmente, uma ou mais das seguintes propriedades do problema conduz à necessidade de empregar o Método Delphi (Linstone e Turoff, 2002):

- O contexto do problema não se adapta a técnicas analíticas precisas, visto que a análise é feita a partir de julgamentos subjetivos numa base coletiva;
- Os indivíduos necessários para contribuir para a análise de um problema complexo não têm histórico de uma comunicação adequada e podem representar diversas realidades quanto à experiência ou grau de conhecimentos;
- Discordâncias entre os indivíduos são tão acentuadas que o processo de comunicação deve ser arbitrado e / ou o anonimato garantido.

Delphi foi inicialmente desenvolvido como um método para aumentar a precisão de previsões. Porém, muitas outras aplicações foram desenvolvidas com base na proposta inicial, como *Policy Delphi* (Linstone e Turoff, 2002) e *Decision Delphi* (Rauch, 1979). Basicamente, *Decision Delphi* é utilizado para estruturar o processo de tomada de decisão, pretendedo-se "criar o futuro" ao invés de apenas fazer previsões. Por outro lado, *Policy Delphi* é uma ferramenta para análise de questões políticas, não é um mecanismo de decisão. Nesta vertente do método, o consenso não é uma meta a ser almejada; pelo contrário, estimula-se a diversidade de opiniões com o fim de garantir que todas as opções e suas possíveis consequências sejam estimadas.

Embora seja um comprovado instrumento de pesquisa, a aplicação tradicional do método não está livre de críticas. Segundo Cooke e Goossens (2004), a análise de problemas a partir do julgamento de especialistas é tipicamente aplicada quando existe incerteza substancial em relação às preferências de um grupo de decisores e seus verdadeiros valores. A aplicação tradicional do método, onde as respostas são dadas em forma de valores pontuais, não fornece qualquer indicação da incerteza de cada entrevistado. Correlacionado com esta questão, as heurísticas e os vieses de comportamento podem influenciar o processo, prejudicando a busca pelo consenso. Outro ponto diz respeito à análise das respostas, visto que a utilização de técnicas pobres de sumarização de resultados pode influenciar o *feedback* dado aos entrevistados, prejudicando a troca de informações e a discussão em torno do consenso.

3.4 ESTIMAÇÃO DE DENSIDADES

A tomada de decisões, mesmo que seja de um grupo, num contexto de incertezas, pode produzir diferentes respostas, dependendo da forma como o processo de decisão é conduzido. Um argumento para minimizar esta questão está voltado para procedimentos que proporcionem respostas por meio de intervalos de valores e que permitam definir uma função (de) densidade de probabilidade (f.d.p.).

O conhecimento da função densidade de probabilidade da variável em estudo permitirá descrever melhor o comportamento esperado para o futuro do processo em causa, contribuindo decisivamente para o processo de tomada da melhor decisão. Inegavelmente uma densidade de probabilidade é desde logo mais informativa do que, por exemplo, a posse de apenas alguns quantis. A estimação de uma densidade é também uma forma mais robusta para a explicação do fenómeno em estudo. Permite lidar melhor com certos aspetos conhecidos e presentes em muitos conjuntos de observações, como caudas e multimodalidade. Pode, por isso, ser mais consistente e concordante com os dados disponíveis.

A função densidade de probabilidade, $f(x)$, é um conceito fundamental em estatística. A sua estimação pode ser feita a partir de uma família paramétrica de modelos, sendo então imposta uma forma a $f(x)$, e, assim, tudo o que resta é estimar os parâmetros da distribuição com base nos dados.

A robustez desta abordagem depende da escolha do modelo paramétrico. Se o modelo designado for o verdadeiro ou próximo deste, as inferências a respeito da distribuição geradora dos dados são plausíveis. No entanto, são impostas restrições sobre a forma que $f(x)$ pode assumir. Por exemplo: uma função de densidade de uma distribuição normal é simétrica e em forma de sino, e consequentemente, inadequada para a representação de densidades bimodais ou assimétricas. Isto pode levar a interpretações inconsistentes do fenómeno em questão.

Uma forma alternativa de tratar o problema está na abordagem não paramétrica. A ideia de uma abordagem não paramétrica é evitar suposições restritivas sobre a forma de $f(x)$, permitindo lidar com um maior número de situações e podendo levar à descoberta de características consideradas insuspeitas aquando da adoção de um modelo paramétrico. A obtenção de uma estimativa da curva da densidade é feita diretamente a partir dos dados, ou seja, “os dados falam por si só”.

De entre as várias metodologias não paramétricas, um importante método para a estimação de funções de densidade de probabilidade é o método do *kernel*. Este permite definir uma curva ou superfície de densidade com identificação visual de áreas com maior probabilidade de ocorrência de um evento. Isso será discutido na próxima secção; maiores detalhes podem ser encontrados em Silverman (1986) ou Carmo (2007).

3.4.1 ESTIMADOR DE DENSIDADE PELO MÉTODO DO *KERNEL*

Seja *X* uma variável aleatória com densidade de probabilidade *f*, que pode ser definida por

$$f(x) = \lim_{h \to 0} \frac{1}{2h} P(x - h < X < x + h)$$

Dado um conjunto de pontos $\{x_1, x_2, ..., x_M\}$ e um valor de *h*, obtém-se uma estimativa para $P(x - h < X < x + h)$ determinando a proporção de observações pertencentes ao intervalo $]x - h, x + h[$. A função densidade de probabilidade empírica pode então ser definida por:

$$\hat{f}(x) = \frac{1}{2hM} \#_{j=1}^{M} \{x_j \in]x - h, x + h[\}$$

ou, equivalentemente,

$$\hat{f}(x) = \frac{1}{Mh} \sum_{j=1}^{M} W\left(\frac{x - x_j}{h}\right)$$

onde

$$W(x) = \begin{cases} 1/2 & \text{se } |x| < 1 \\ 0 & \text{caso contrário} \end{cases}$$

Podemos observar que $\hat{f}(x)$ não é uma função contínua e tem derivada nula em todos os pontos, exceto nos pontos de "salto" $x_j \pm h$.

Um estimador de densidades contínuas pode ser obtido substituindo a função de ponderação *W* por uma função contínua não negativa *K*, denominada função *kernel*, ou função *núcleo*, satisfazendo a condição

$$\int_{-\infty}^{+\infty} K(x)\, dx = 1$$

O chamado método do *kernel* — para estimação dita "não paramétrica" de densidades — consiste, então, em aproximar a densidade de probabilidade da seguinte forma:

$$\hat{f}(x) = \frac{1}{Mh}\sum_{j=1}^{M} K\left(\frac{x - x_j}{h}\right)$$

onde h é um parâmetro de dispersão e K é a função *kernel*. Em geral, esta é, por si só, uma função densidade de probabilidade relativamente simples, sendo as mais usadas a Retangular, a Triangular, a Logística e, sobretudo, a Gaussiana. Isto garante que $\hat{f}(x)$ também seja uma função densidade. Além disso, a forma de composição aditiva assegura que $\hat{f}(x)$ contenha as mesmas propriedades de continuidade e diferenciabilidade de K (Silverman, 1986).

O método do *kernel* pode ser visto como uma média aritmética simples de curvas centradas nas observações. O contorno da curva resultante pode ser mais irregular ou mais suave, dependendo da função *kernel* escolhida e, sobretudo, do valor escolhido para h. A Figura 3.2, adaptada de Carmo (2007), ilustra o efeito do valor escolhido para o raio na composição de $M = 8$ funções *kernel* gaussianas.

No que se segue, consideraremos que dispomos de uma discretização da função densidade de probabilidade estimada, isto é, da avaliação da função $\hat{f}$ num conjunto de pontos $S = \{s_1, s_2, ..., s_N\}$, sendo conveniente que estes estejam regularmente espaçados $(s_{j+1} - s_j = \Delta)$, sejam em número suficientemente grande, e que o intervalo $[s_1, s_N]$ seja judiciosamente escolhido.

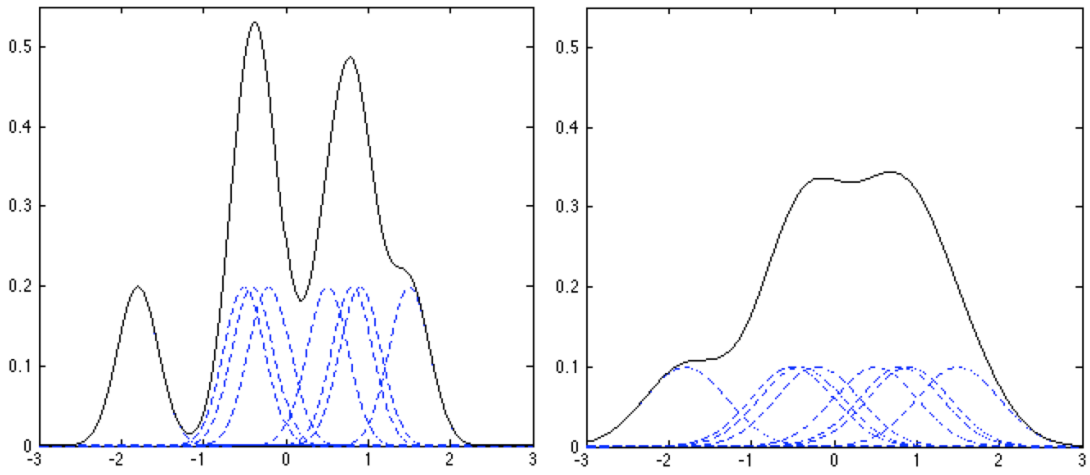


Figura 3.2 - Estimativas de uma densidade pelo método do *kernel* usando curvas gaussianas e para diferentes escolhas do parâmetro de dispersão: (a) *h*=0.25; (b) *h*=0.5

3.4.2 ESTIMAÇÃO DE QUANTIS

A partir de $\left\{\hat{f}(s_i)\right\}$, é fácil obter, por integração numérica, uma estimativa discretizada da função distribuição de probabilidade, $\left\{\hat{F}(s_i)\right\}$. Para esse efeito, consideraremos a bem conhecida Regra do Trapézio, que considera a aproximação de $f(x)$ definida pela linha poligonal contínua que passa pelos pontos $\left\{\left(s_i, \hat{f}(s_i)\right)\right\}_{i=1,\ldots,N}$:

$$\hat{F}(s_{j+1}) - \hat{F}(s_j) = \frac{\Delta}{2}\left[\hat{f}\left(s_j\right) + \hat{f}\left(s_{j+1}\right)\right]$$

Dispondo de $\hat{F}$, é fácil obter estimativas para quaisquer quantis de probabilidade que seja necessário calcular. Recorde-se que o quantil de probabilidade θ de uma variável aleatória contínua X é o valor q_θ de X para o qual a função de distribuição de X tem valor θ:

$$F\left(q_\theta\right) = P\left(X \le q_\theta\right) = \theta$$

Em geral, dada uma probabilidade θ, é fácil identificar qual o intervalo $\left[s_j, s_{j+1}\right]$, tal que $\hat{F}(s_j) \le \theta < \hat{F}(s_{j+1})$. Sendo Δ suficientemente pequeno, pode-se então simplesmente considerar $\hat{q}_\theta = s_j$, ou $\hat{q}_\theta = \left(s_j + s_{j+1}\right)\big/2$.

3.5 PROCEDIMENTO PROPOSTO: MÉTODO DELPHI INTERVALAR

O método Delphi é essencialmente um procedimento empírico e não está baseado em qualquer procedimento matemático mais profundo. A sua aplicação tradicional pode ignorar e não explorar pontos de discordância entre as respostas levantadas devido à utilização de técnicas pobres de sumarização dos resultados. Outra questão, referida anteriormente, diz respeito ao facto de, na aplicação tradicional do método, a resposta de cada indivíduo entrevistado ser dada sob a forma de um valor singular, não fornecendo qualquer indicação sobre o grau de incerteza que ele deposita na resposta. Finalmente, como sugerido por Von Der Gracht (2012), os investigadores devem ter em mente que, além de estatísticas de consenso, outras análises, tais como gráficos de dispersão, as

análises de subgrupos, ou análises de impacto, também podem levar a resultados interessantes em estudos onde é utilizado o Delphi.

Sendo assim, em função das características do problema principal abordado neste trabalho, avaliação do risco de segurança para proteção de portos, fazemos uma proposta de um método intitulado **método Delphi Intervalar.** O método pretende proporcionar aos participantes, tanto no processo de elicitação de preferências quanto na elicitação das opiniões de especialistas, uma visão abrangente, uma vez que leva em consideração todos os aspetos mencionados anteriormente neste capítulo. As principais características do método são ressaltadas a seguir:

- Possui as mesmas fases do método Delphi tradicional apresentadas na Figura 3.1;
- Os entrevistados fornecem as suas opiniões ou preferências através de intervalos de valores em vez de valores pontuais;
- A cada intervalo é associada uma função densidade *kernel*, que permite graduar a incerteza das respostas;
- As densidades dos diferentes entrevistados são posteriormente combinadas, dando origem a uma nova f.d.p. pela aplicação do método descrito na Secção 3.4;
- O coordenador possui a liberdade de atribuir diferentes pesos aos entrevistados com o objetivo de conduzir o grupo a uma situação de consenso;
- O *feedback* dado aos entrevistados consiste na apresentação do gráfico da função de densidade de probabilidade estimada e os quantis das respostas;
- A obtenção de uma f.d.p. unimodal e simétrica pode ser interpretada como uma forma representativa de algum consenso, sendo depois desejável a redução da dispersão nessa f.d.p.

Apresentamos na Figura 3.3, em forma esquemática, as fases do método Delphi Intervalar, para efeito de comparação com o método Delphi tradicional.

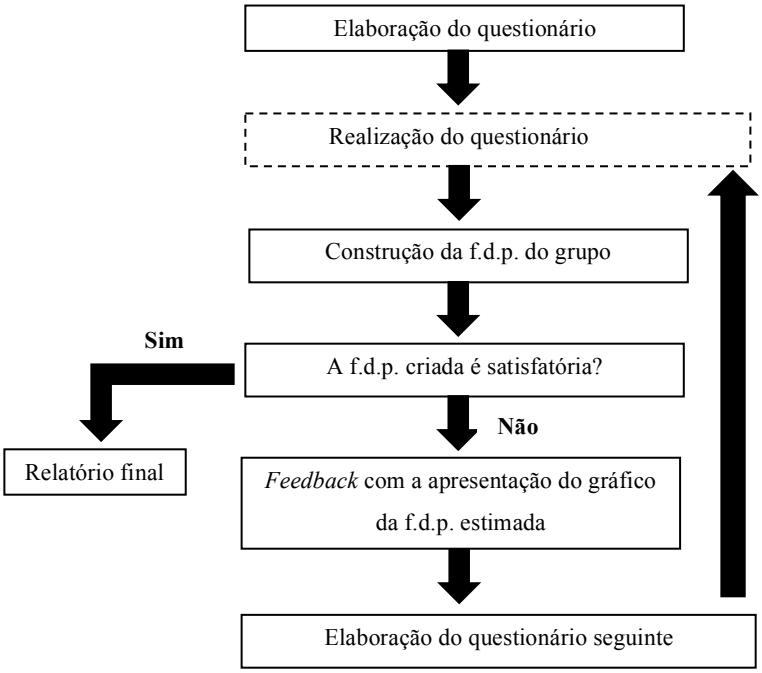


Figura 3.3 - Fases do método Delphi Intervalar

3.5.1 RESPOSTAS INTERVALARES

Usualmente, o método Delphi tradicional considera respostas pontuais as perguntas do questionário, mas, em vez disso, pode ser obtida mais informação sobre o grau de incerteza, solicitando-se ao decisor uma resposta em forma de um intervalo numérico, sem um acréscimo substancial de dificuldade para o mesmo. Assim, obtêm-se duas estimativas ou dois parâmetros das preferências, os extremos do intervalo respetivo. A este intervalo é associada uma função densidade de probabilidade.

No entanto, respostas em forma de intervalos, frequentemente, podem mostrar um excesso de confiança; a literatura apresenta exemplos que são características desse fenómeno de comportamento. Alguns deles são associados ao facto de que o excesso de confiança pode aumentar com a disponibilidade de informações, ou de que aumenta à medida de que as perguntas se tornam mais difíceis, ou simplesmente está relacionado com o estilo cognitivo das pessoas (O'Hagan *et al.*, 2006). Outro campo de investigação tem enfatizado que o grau de excesso de confiança pode variar dependendo da forma como os intervalos são elicitados (Soll e Klayman, 2004; Speirs-Bridge *et al.*, 2010).

Essas investigações têm como intuito desenvolver um processo de elicitação que minimize o grau do excesso de confiança das estimativas e foram conduzidas em contextos bastante diferentes dos que são aqui discutidos. Estudar o desempenho dos especialistas em

perguntas de um domínio específico pode ajudar na compreensão do excesso de confiança como um fenómeno psicológico geral. Porém, esses conjuntos de dados, provenientes da análise de domínios específicos, não serão necessariamente representativos dos tipos de perguntas para as quais queremos usar as opiniões de especialistas e, também, as potencias preferências dos decisores, no problema discutido neste trabalho.

Independentemente do contexto, uma dificuldade inerente a qualquer elicitação é alusiva ao facto de o entrevistado não ser capaz de especificar qualquer valor — seja uma preferência, uma estimativa pontual, intervalar ou uma probabilidade — com absoluta precisão. Sendo assim, iremos considerar as estimativas intervalares como representação de um intervalo de confiança de 90%. Esta abordagem é defendida no trabalho de Moder e Rodgers (1968), onde, num estudo referente ao método PERT, os extremos dos intervalos elicitados são interpretados como estimativas dos percentis $q_{0,05}$ e $q_{0,95}$, e por Teigen e Jørgensen (2005), que, a partir de várias experiências, concluíram que os julgamentos são razoavelmente mais corretos, e com níveis de excesso de confiança reduzidos, quando é atribuído um intervalo de confiança às respostas.

Sem prejuízo de outras funções *kernel* poderem ser consideradas, associamos uma função de densidade de probabilidade Normal ao intervalo, sendo esta centrada no ponto médio do intervalo e tendo dispersão definida pelos quantis 5% e 95%, conforme Figura 3.4.

O uso da densidade Normal como forma de avaliar as incertezas e imprecisões em elicitações não é novidade: a literatura apresenta diversos trabalhos sobre esta abordagem, como os de Winkler (1981) e Garthwaite *et al.* (2005).

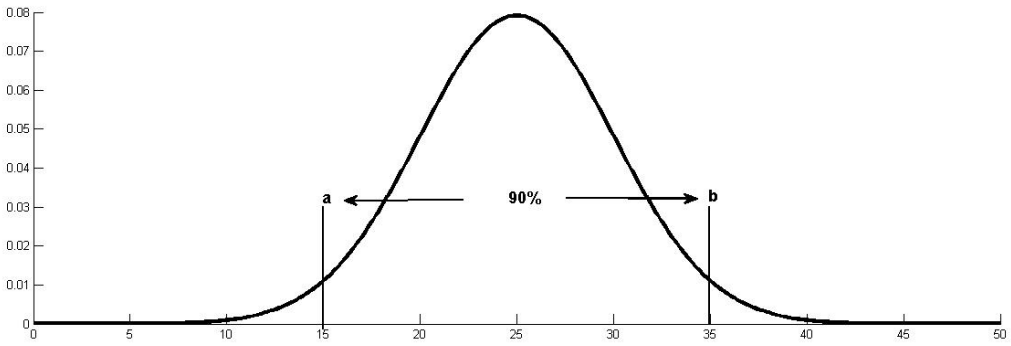


Figura 3.4 - Função de densidade Normal atribuída a cada estimativa intervalar

No entanto, levanta-se o problema de como adequar a curva gaussiana às estimativas intervalares quando a quantidade a ser estimada está naturalmente definida só num semieixo ou até num intervalo limitado (como, por exemplo, uma probabilidade). Devido ao suporte da distribuição Normal ser o conjunto dos números reais, há sempre um certo valor de probabilidade que poderá ficar fora do domínio de admissibilidade e que poderá ou não ser reconhecido como negligenciável. Uma possibilidade seria o emprego explícito de truncatura, com correção do efeito produzido por esse procedimento. O mesmo problema poderia surgir caso fosse considerada uma função *kernel* com suporte limitado — Galway (2007) discute-o no caso do ajustamento de uma f.d.p. Triangular, também supondo que as estimativas fornecidas devem representar um intervalo de confiança de 90%. Note-se que, nesse caso, é necessário que os entrevistados forneçam uma resposta suplementar, correspondente ao valor modal da Triangular. Não serão aqui discutidos em pormenor, quaisquer possíveis procedimentos corretivos. Na verdade, acreditamos que os excedentes de probabilidade atrás referidos podem, em geral, ser considerados negligenciáveis. Esses efeitos são naturalmente atenuados, quer por resultado da combinação de várias densidades, quer devido à expectável redução da dispersão na sucessão de rondas do processo de elicitação proposto.

Em seguida, apresentamos sob a forma de algoritmo o conjunto de procedimentos do método proposto.

Algoritmo 1: Método Delphi Intervalar

Sejam:

$J = \{1,2,...,M\}$: conjunto dos entrevistados

S: conjunto dos pontos (regularmente espaçados) onde é feita a avaliação das densidades

$k = 0$;

REPETIR:

$k = k + 1$ (nova ronda)

Recolher as estimativas intervalares,

$$\left\{\left(a_{kj}, b_{kj}\right)\right\}_{j \in J}$$

Calcular os indicadores de localização e dispersão,

$$\mu_{kj} = \frac{a_{kj} + b_{kj}}{2} \quad \text{e} \quad \sigma_{kj} = \frac{b_{kj} - \mu_{kj}}{1.645}$$

Calcular as funções *kernel* individuais,

$$\left\{f_{kj}(s)\right\}_{j \in J,\, s \in S} \quad \text{com} \quad f_{kj} \sim N\left(\mu_{kj}, \sigma_{kj}\right)$$

Calcular os pesos a atribuir aos entrevistados,

$$\left\{w_{kj}\right\}_{j \in J}$$

Calcular estimativas da densidade de probabilidade agregada,

$$\left\{\hat{f}_k(s)\right\}_{s \in S}, \ \text{com} \ \ \hat{f}_k(s) = \sum_{j \in J} w_{kj} f_{kj}(s)$$

SAIR SE ficar satisfeita uma condição de paragem apropriada

Apresentar $\hat{f}_k$ aos entrevistados (representação gráfica)

Calcular e apresentar a média de $\hat{f}_k$ (e possivelmente outros indicadores)

A condição de paragem do processo é suscetível de ser definida de forma objetiva, mas várias possibilidades podem ser consideradas, a começar pela simples pré-definição do número de rondas a realizar, por exemplo, 3. Outra alternativa simples consiste em parar quando o valor da média de $\hat{f}_k$ não diferir significativamente da média de $\hat{f}_{k-1}$. Por outro lado, é desejável que a densidade final tenha características relativamente próximas da gaussianidade — em especial, unimodalidade e simetria —, e idealmente com dispersão relativamente reduzida.

3.5.2 IMPORTÂNCIA DOS ENTREVISTADOS

O método Delphi Intervalar também visa contornar a influência exagerada que a resposta de um entrevistado ou de uma minoria de entrevistados poderia ter no processo de elicitação e agregação em sobreposição à maioria. O fator "influência" poderia ser minimizado ao se garantir o anonimato dos entrevistados, porém, este anonimato não evita outros problemas: os participantes de um painel Delphi podem ignorar o *feedback* das respostas e responder da mesma forma que na ronda anterior devido à relutância em fazer mudanças, ou podem, até, afastar-se propositadamente das respostas restantes do grupo. Por este motivo, muitas vezes é necessário influenciar individualmente os membros do grupo, com o objetivo de construir uma decisão de consenso. Nesta situação, o coordenador do processo precisar ser alguém que saiba lidar com questões vinculadas ao comportamento humano, com a finalidade de ajudar um grupo de pessoas a compreender os seus objetivos comuns e a planear a forma de alcançá-los, sem, no entanto, tomar uma posição particular na discussão. O papel do coordenador é muito importante para ajudar à aproximação de posições, mas nem sempre é fácil ou defensável influenciar o comportamento dos elementos de um grupo, com o objetivo de construir uma solução de maior consenso.

A nossa proposta permite a um coordenador atribuir pesos, w_{kj}, aos entrevistados em função das respostas intervalares geradas a partir da análise da qualidade das respostas individuais.

Segundo Silverman (1986), no clássico método do *kernel* para estimação não paramétrica de densidades, as estimativas

$$\hat{f}_k(x) = \sum_{j \in J} w_{kj} f_{kj}(x)$$

recorrem a pesos iguais e imutáveis:

$$w_{kj} = 1/M \qquad \textbf{(3.1)}$$

Contudo, há várias razões que podem ser invocadas para usar pesos diferentes, por entrevistado e/ou por ronda. Em primeiro lugar, refira-se que, nalgumas situações, poderão estar disponíveis medidas de mérito indicativas do grau de acerto dos entrevistados em inquéritos formalmente semelhantes realizados anteriormente e para os quais seja conhecido o valor exato da quantidade a ser estimada subjetivamente. Esse tipo de exercício pode ser útil na preparação, aferição e calibração dos entrevistados. Por outro

lado, pode estar definido à partida — justa ou injustamente — um crédito maior ou menor dos entrevistados com base no seu *status* ou grau de responsabilidade.

Para além desses pesos definidos *a priori*, é natural considerar pesos diferentes a partir das respostas dadas durante o próprio processo de elicitação. Por exemplo, pode-se argumentar que, em geral, um intervalo de maior amplitude merece maior credibilidade do que um intervalo demasiado reduzido. Outra abordagem consiste em atribuir maior ou menor peso às respostas individuais consoante estejam mais próximas ou mais afastadas da mediana do grupo. Concretamente, estes pesos podem ser calculados, em cada ronda, da seguinte forma:

$$\begin{aligned} &\tilde{x}_k = \text{mediana de } \mu_{kj} \\ &d_{kj} = \left\{\left|\mu_{kj} - \tilde{x}_k\right|\right\} \quad \text{(avaliação das distâncias)} \\ &v_{kj} = \frac{1}{d_{kj}+1} \qquad \text{(graduação)} \\ &w_{kj} = \frac{v_{kj}}{\sum_i v_{kj}} \qquad \text{(normalização)} \end{aligned} \tag{3.2}$$

Por exemplo, com $\left\{d_{kj}\right\}_j = \{0,1,2,3,10\}$, os pesos resultantes seriam:

$$\left\{w_{kj}\right\}_j = \{0.460, 0.230, 0.153, 0.115, 0.042\}.$$

Nota-se, a partir do exemplo, que o efeito desejado consiste em atribuir maiores pesos às respostas com as menores distâncias entre as suas médias e a tendência central do grupo e menores pesos no caso contrário. Este procedimento não ignora nenhum entrevistado, mas bonifica sobremaneira as respostas mais "centrais", o que resulta numa densidade $\hat{f}_k$ com menor dispersão. Por outras palavras, induz artificiosamente uma aproximação de posições, que os entrevistados poderão ou não querer contrariar na ronda seguinte.

Outra ideia poderia consistir em definir uma repartição mais equilibrada para a definição dos pesos da seguinte forma:

$$\mathrm{v}_{kj} = \frac{\left(\max d_{kj}\right) - \left(d_{kj}\right)}{\left(\max d_{kj}\right) - \left(\min d_{kj}\right)} \tag{3.3}$$

Nesse procedimento, a resposta mais distante da mediana do grupo é simplesmente ignorada, independentemente de ter características de *outlier* estatístico, ou não. As restantes teriam pesos mais equilibrados, uma vez que decrescem de forma linear.

Para os mesmos valores do exemplo acima, $\{d_{kj}\}_j = \{0,1,2,3,10\}$, resultaria, respectivamente,

$$\{w_{kj}\}_j = \{0.294, 0.265, 0.235, 0.206, 0\}.$$

3.6 EXEMPLOS ILUSTRATIVOS

Nesta secção, dois estudos de caso são usados com o objetivo de explicitar o **Método Delphi Intervalar** proposto. Neles, foram consultados, respetivamente, alunos do curso de mestrado em Estatística e Investigação Operacional da Faculdade de Ciências da Universidade de Lisboa e analistas da Divisão de Pesquisa Operacional do Centro de Análises de Sistemas Navais (CASNAV) — órgão de ciência, tecnologia e inovação da Marinha do Brasil.

Para o efeito, foi utilizado um projeto de interface gráfica desenvolvido em ambiente MATLAB para facilitar a comunicação e o processo de *feedback* com os entrevistados — vide Figura 3.5. A tela da interface possibilita ao entrevistado inserir um intervalo que corresponde à resposta de cada pergunta. Os limites do intervalo são os percentis 0.05 e 0.95, conforme referido na Subsecção 3.4.1. A escolha destes limites pode ser feita movendo as pegas de um *slider* duplo ou, diretamente, inserindo-se os valores nas caixas de diálogo ao lado de cada *slider*.

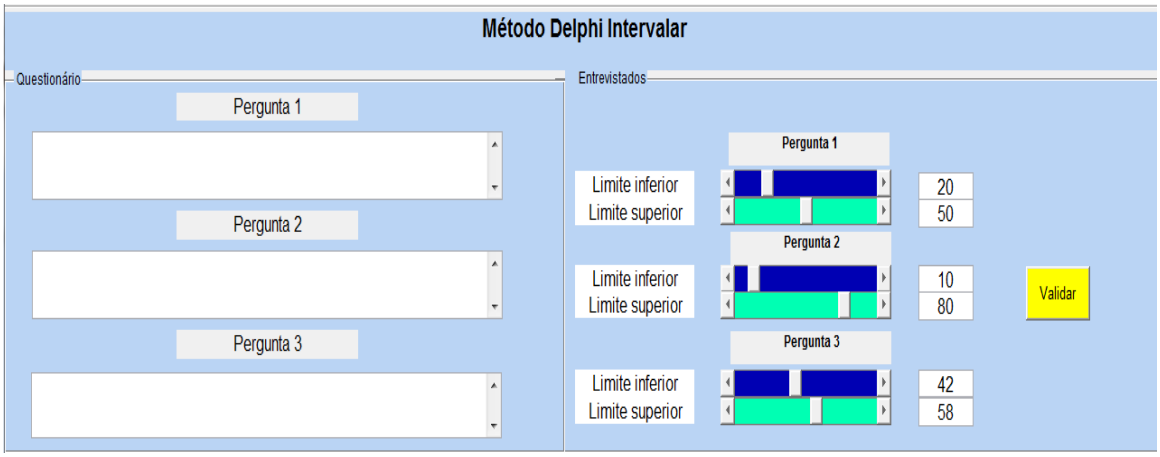


Figura 3.5 - Tela da interface gráfica com os objetos gráficos utilizados pelos entrevistados

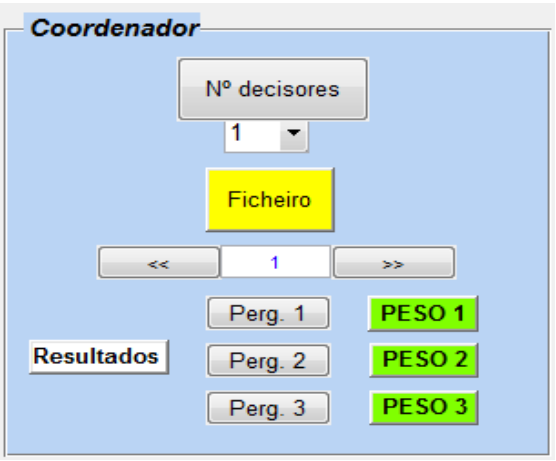


Figura 3.6 - Tela da interface gráfica com os objetos gráficos utilizados pelo coordenador

Seguindo as etapas do método, tornou-se também necessária a criação de um painel para o coordenador (Fig. 3.6). Neste painel, o coordenador deve definir o número de decisores (entrevistados), valor este que irá definir o tamanho das matrizes com as respostas geradas por cada entrevistado e que ficarão armazenadas. Os botões **PESO 1, 2 e 3** permitem ao coordenador aplicar pesos aos entrevistados de acordo com as formulações — Eqs. 3.1, 3.2 e 3.3, respetivamente — apresentadas na Subsecção 3.5.2. Posteriormente, ao se clicar nos botões **Perg. 1, Perg. 2** ou **Perg. 3** são apresentados, no quadro de *feedback* aos entrevistados, os gráficos da funções de densidade de probabilidade do grupo referentes às respetivas perguntas, de acordo com o método do *kernel* explicitado na Secção 3.4.

A Figura 3.7 ilustra o quadro de *feedback* aos entrevistados disponibilizado pela interface gráfica. O quadro apresenta o gráfico de uma hipotética função de densidade de probabilidade de um grupo, além da mediana, 1º quartil e 3º quartil dessa densidade.

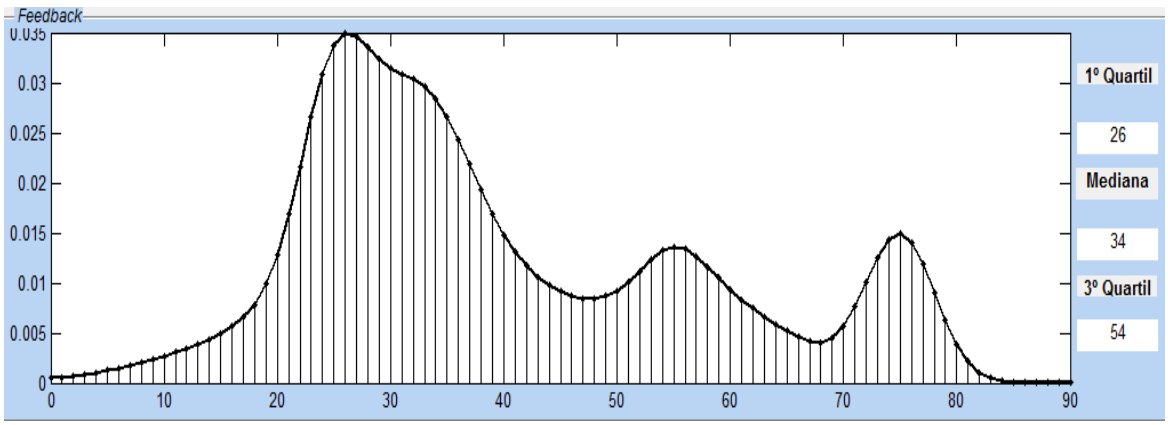


Figura 3.7 - Painel de *feedback* aos entrevistados

3.6.1 PRIMEIRO ESTUDO DE CASO

O primeiro caso refere-se a uma situação hipotética e tinha por objetivo capturar o grau de atenção dos alunos durante a experiência, abordando um assunto que faz parte do quotidiano das pessoas: considere que durante um passeio numa bela tarde de domingo, você é abordado por um funcionário de um instituto de estatística que faz uma pesquisa sobre a opinião dos jovens portugueses sobre a idade que eles consideram como ideal para o casamento: "*dê a sua opinião a respeito da idade que considera ideal para o casamento na forma de um intervalo de valores*".

Os intervalos escolhidos por cada entrevistado j na primeira ronda ($k = 1$) são apresentados na Tabela 3.1, enquanto a Figura 3.8 representa as funções *kernel* de cada entrevistado com as respetivas médias e desvios-padrão.

A Figura 3.9 representa o quadro de *feedback* aos entrevistados na interface gráfica implementada. Na figura podemos ver a função de densidade de probabilidade do grupo, que foi definida atribuindo-se iguais pesos aos entrevistados.

Tabela 3.1 - Intervalos fornecidos pelos entrevistados

Entrevistado	Intervalo
J_1	[26, 34]
J_2	[21, 35]
J_3	[27, 37]
J_4	[20, 30]
J_5	[25, 35]
J_6	[23, 35]
J_7	[25, 30]
J_8	[28, 34]
J_9	[26, 34]

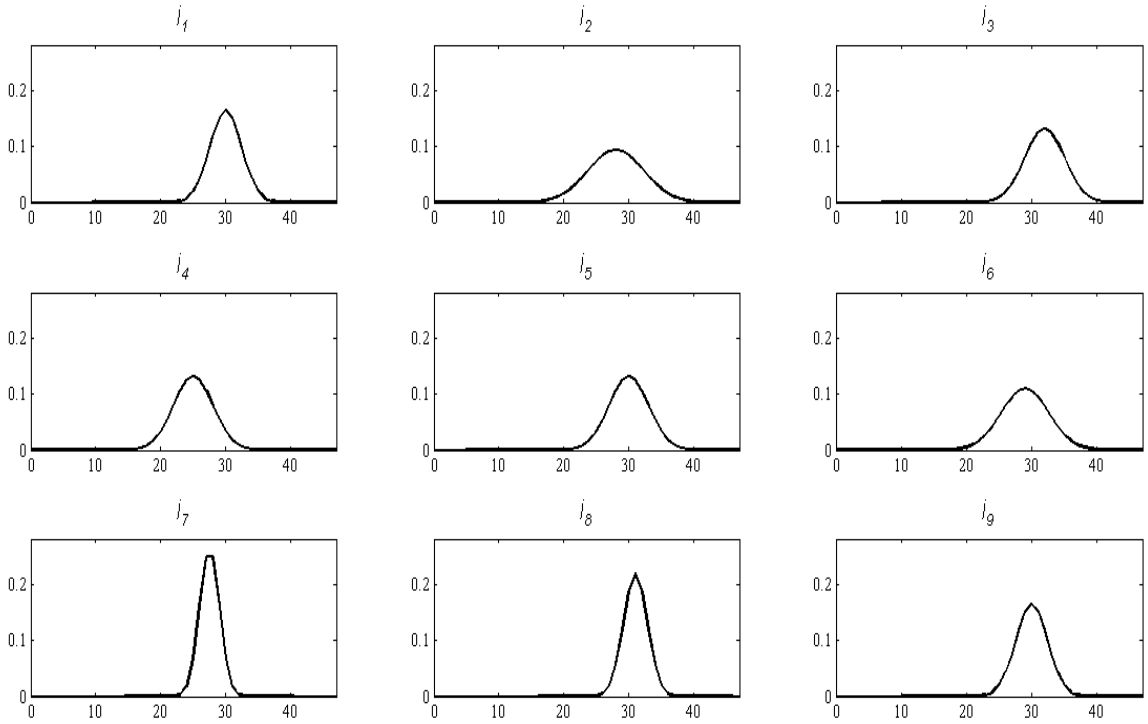


Figura 3.8 - Funções de densidade de probabilidade de cada entrevistado

Observa-se que a densidade estimada na Figura 3.9 apresenta uma forma unimodal, simétrica e com uma dispersão relativamente reduzida, isto se deve ao fato de que os intervalos de valores de cada entrevistado não apresentaram grandes diferenças entre si. Portanto, na experiência realizada em sala de aula não foi considerada necessária uma 2ª ronda de perguntas e respostas. Um relativo consenso foi logo alcançado na 1ª ronda, considerando-se o intervalo interquartil de [26, 32] como o período ideal para o casamento.

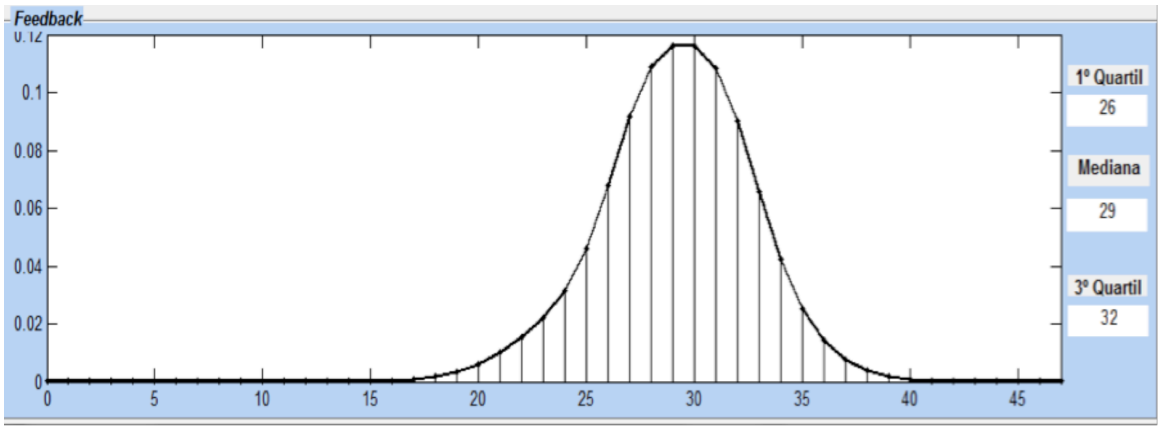


Figura 3.9 - Densidade estimada pelo método do *kernel* a partir da agregação das densidades apresentadas na Fig. 3.8

Este estudo de caso não possui qualquer relação com a problemática de avaliação de riscos de segurança contra ameaças terroristas, foco principal deste trabalho. O objetivo foi, somente, apresentar o método aos alunos e ilustrar a sua aplicação, abordando um assunto de fácil entendimento. Contudo, uma mesma pergunta pode ser interpretada de forma diferente pelos indivíduos consultados, pelo que introduzimos uma pequena discussão sobre dificuldades comuns em sondagens — isto é, como evitar que as respostas dos entrevistados dependam do formato da consulta ou da formulação das perguntas. Em particular, há que prevenir possíveis ambiguidades.

Como dito no início desta subsecção, a proposta da pergunta era pedir aos alunos uma opinião para a idade que consideram ideal para o casamento, esperando que as respostas fossem interpretadas como **estimativas**. Contudo, essa pergunta pode ser interpretada de formas diferentes. O entrevistado J_1, por exemplo, tanto pode pensar:

a) Idealmente uma pessoa devia casar-se entre os 26 e os 34 anos, antes disso é muito cedo e depois é muito tarde;
b) Existe uma idade considerada ideal para se casar, que não sei bem qual é, mas acho que está entre 26 e 34.

Caso tenha interpretado como (a), o aluno pode ter seguido um modelo de racionalidade de carácter normativo ou de carácter prescritivo. Os modelos normativos pretendem ser universais, visam determinar um rumo de ação ideal para todos, dado um conjunto de circunstâncias. Por analogia, podemos considerar as normas éticas e religiosas e as leis (Dias e Tsoukiàs, 2004). No caso de ter seguido um modelo de carácter prescritivo, o aluno visou produzir um rumo de ação ideal para uma entidade (pessoa ou organização), tendo em conta as circunstâncias específicas dessa entidade — no caso, o que seria pessoalmente melhor para um solteiro ou, em particular, para ele próprio.

Em relação à interpretação (b), os modelos de raciocínio que podem ter sido seguidos são os de carácter descritivo ou preditivo. Os modelos descritivos dizem respeito a como as pessoas pensam e agem na realidade, e ao que realmente acontece — qual a idade com que, de facto, os jovens portugueses se casam. Caso o aluno tenha raciocinado de forma a fazer uma previsão do que acontecerá ao se projetar a vida de um jovem, ou seja, uma estimativa, ele seguiu um modelo de natureza preditiva.

De qualquer forma, embora a pergunta apele a uma opinião sobre os "outros", a resposta está inevitavelmente contaminada pelas vontades, planos ou desejos do entrevistado em relação à sua vida pessoal. Sendo assim, para evitar essas ambiguidades, sugerimos que será melhor decompor uma pergunta em várias e definir como devem ser

respondidas, de forma a proporcionar ao entrevistado uma melhor compreensão do que está a ser perguntado e para que a análise possa até beneficiar da maior riqueza de respostas — exemplo:

(Q1)

(a) "Qual é o seu candidato preferido?";

(b) "Qual é a percentagem de votos que acha que esse candidato vai obter?";

(Q2)

(a) "Qual é o candidato que você acha, realisticamente, que vai vencer?";

(b) "Qual é a percentagem de votos que acha que esse candidato vai obter?".

Note-se que as questões (a) são respondidas em escalas nominais, enquanto as questões (b) são respondidas em escalas numéricas de proporção, o que permitirá realizar análises estatísticas com maior valor informativo.

Existe alguma redundância no conjunto de perguntas, que pode, até, ser benéfica, de modo a eliminar respostas inconsistentes.

3.6.2 SEGUNDO ESTUDO DE CASO

Este estudo de caso aproxima-se do contexto do problema do risco de segurança em portos e tinha por objetivo capturar o grau de consenso dos entrevistados em relação à importância dos atributos que devem ser levados em consideração num processo de avaliação de riscos:

"Suponha que você faz parte de um grupo de autoridades responsável pela segurança do porto do Rio de Janeiro. A administração do porto considera que os atributos Impacto Ambiental, Impacto Económico e Impacto Social são relevantes na avaliação das consequências de um eventual ataque terrorista. As medidas de proteção a tomar irão depender dos 'pesos' (graus de importância) para os atributos que resultem da combinação das opiniões de todos os elementos deste grupo. Para tentar fomentar uma convergência de opiniões, será usada a metodologia antes exposta. Em cada ronda do processo, deve dar a sua opinião pessoal, indicando qual o grau de importância que reconhece, com maior ou menor convicção, a cada atributo. Assim, cada resposta deverá ser traduzida por um intervalo de valores dentro da escala 0 a 100."

Recorde-se que um dos objetivos do método é representar as incertezas das preferências ou estimativas dos entrevistados através de funções de densidade de probabilidade. Note-se que, neste exemplo, a pretensão foi concluir por avaliações dos

atributos, em valor absoluto, sem levar em consideração outros aspetos, nomeadamente, correlações entre os mesmos.

Foram realizadas duas rondas de perguntas com os analistas da divisão de Pesquisa Operacional do CASNAV. Nesta experiência, foram aplicados todos os procedimentos antes apresentados para a definição de pesos aos entrevistados, e os respectivos resultados apresentados aos mesmos, de forma a ilustrar as diferenças de forma das densidades resultantes e, possivelmente, facilitar até o alcance de um consenso.

Na Tabela 3.2 encontram-se os intervalos de valores respondidos por cada entrevistado, na 1ª ronda de consultas, relativamente à importância dos atributos Impacto Ambiental, Económico e Social.

A Figura 3.10 apresenta os gráficos das funções *kernel* de cada entrevistado.

A Figura 3.11 ilustra os quadros de *feedback* aos entrevistados relacionados com a definição da importância do critério Impacto Ambiental. A figura mostra as 3 funções de densidade de probabilidade resultantes da aplicação dos 3 procedimentos — Eqs. 3.1, 3.2 e 3.3, respetivamente — para a definição de pesos para os intervalos fornecidos pelos entrevistados.

Tabela 3.2 - Intervalos definidos pelos entrevistados para os atributos Impacto Ambiental, Económico e Social na 1ª ronda de perguntas

Entrevistado	Impacto Ambiental	Impacto Económico	Impacto Social
J_1	[30, 70]	[50, 90]	[70, 100]
J_2	[40, 70]	[60, 90]	[60, 90]
J_3	[50, 60]	[70, 90]	[50, 70]
J_4	[30, 60]	[40, 60]	[60, 80]
J_5	[50, 70]	[60, 70]	[80, 90]
J_6	[70, 80]	[30, 50]	[30, 50]
J_7	[20, 30]	[80, 100]	[60, 80]
J_8	[25, 40]	[70, 100]	[50, 70]
J_9	[10, 50]	[50, 80]	[90, 100]

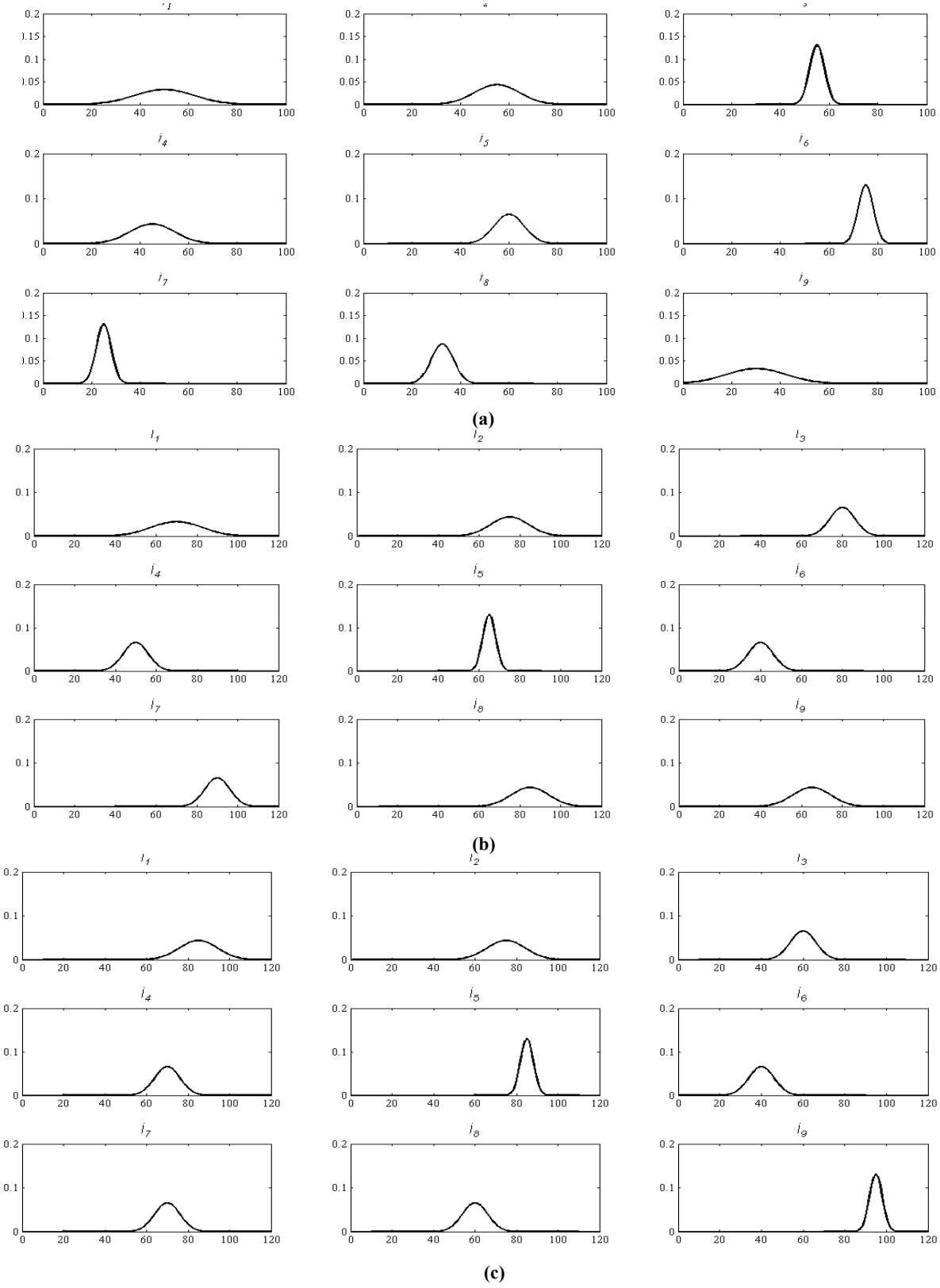
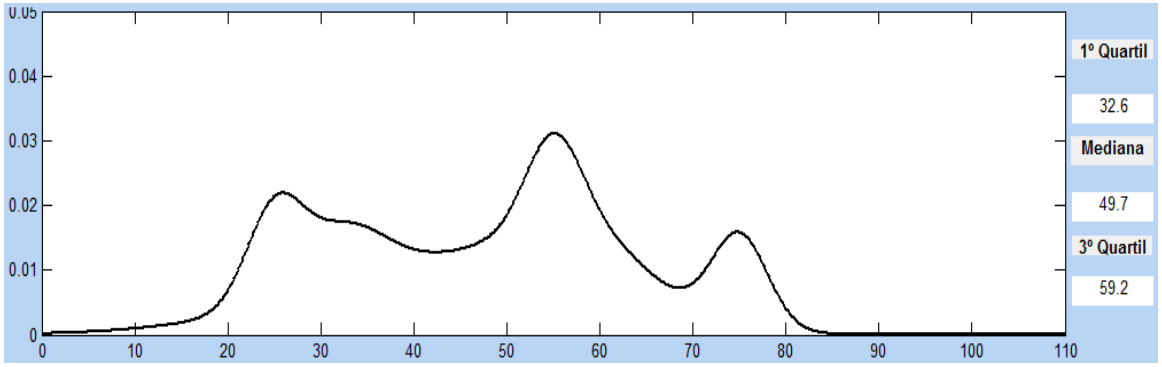
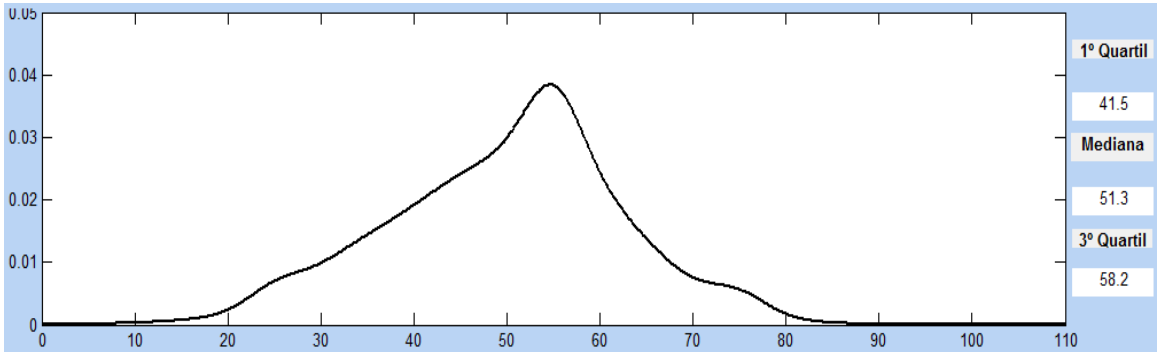


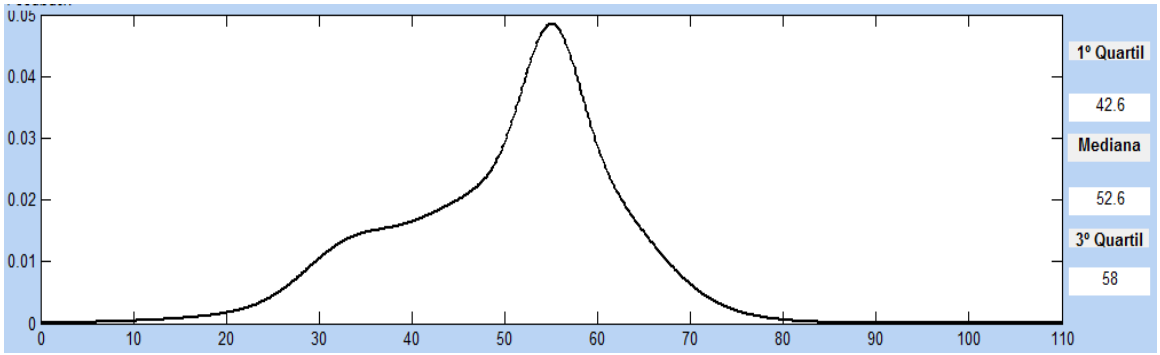
Figura 3.10 - Funções de densidade de probabilidade Normais de cada entrevistado para os atributos: (a) Impacto Ambiental; (b) Impacto Económico; (c) Impacto Social



(a)



(b)



(c)

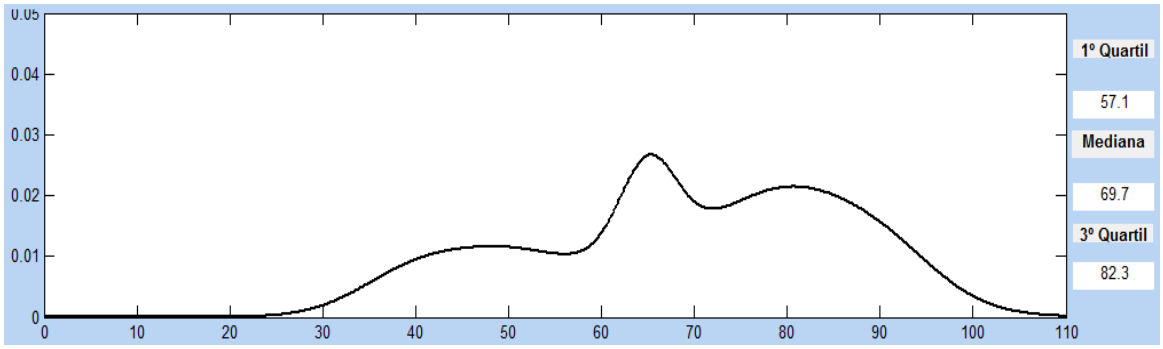
Figura 3.11 - Densidades geradas para o atributo Impacto Ambiental ao se atribuir pesos aos entrevistados: (a) Eq. 3.1; (b) Eq. 3.2; (c) Eq. 3.3

A Fig. 3.11(a) mostra o gráfico da função de densidade gerada atribuindo-se iguais pesos a cada entrevistado. Observamos as seguintes características: densidade multimodal e dispersão relativamente elevada, com um intervalo interquartil de 26.6 pontos. Podemos concluir que o consenso estaria longe de ser alcançado. Ao aplicar-se a formulação da Eq. 3.2, ilustrado no quadro de *feedback* em (b), a mediana do grupo sofre uma pequena alteração e o intervalo interquartil é reduzido para 16.7 pontos. Além disso, a função torna-se unimodal, uma vez que exibe apenas um máximo local. Características não

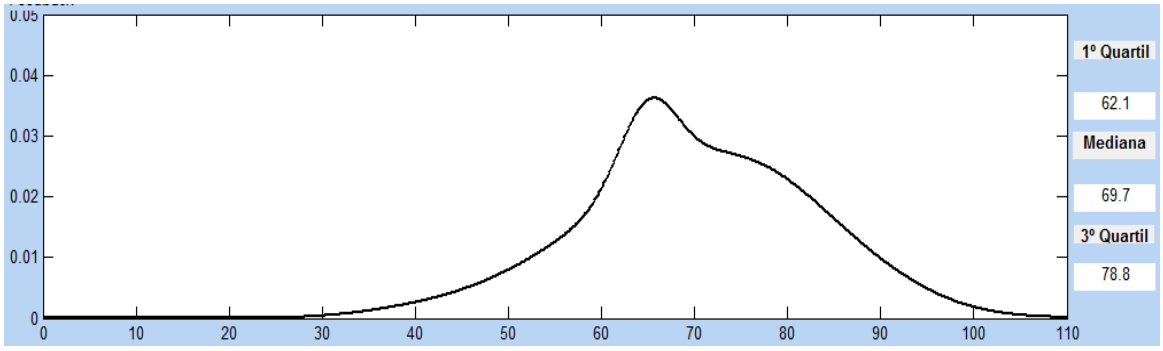
muito diferentes são observadas com a aplicação da Eq. 3.3 para a definição de pesos aos entrevistados.

Os quadros de *feedback* com os gráficos das funções de densidade conjunta para os outros dois atributos são mostrados nas Figuras 3.12 e 3.13.

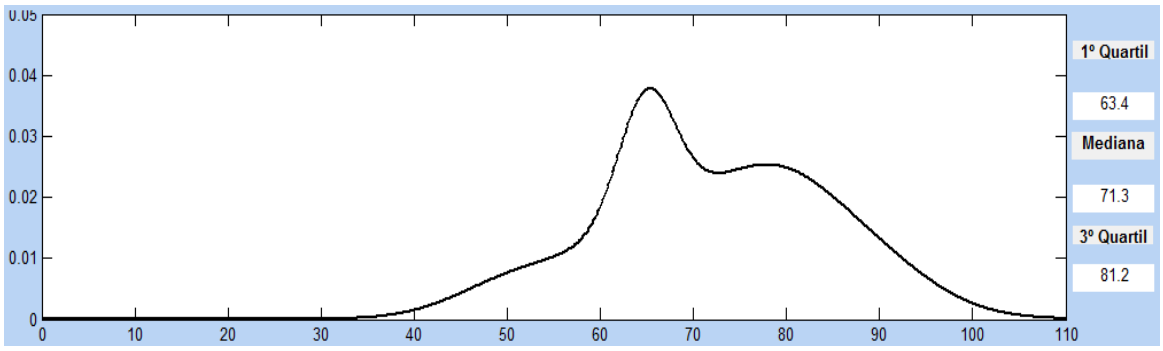
Em geral, mantêm-se as características antes observadas relativamente ao atributo Impacto Ambiental. No entanto, agora observa-se que o procedimento da Eq. 3.3 não reduz tão drasticamente a multimodalidade presente na densidade conjunta que resulta do procedimento básico, da Eq. 3.1.



(a)

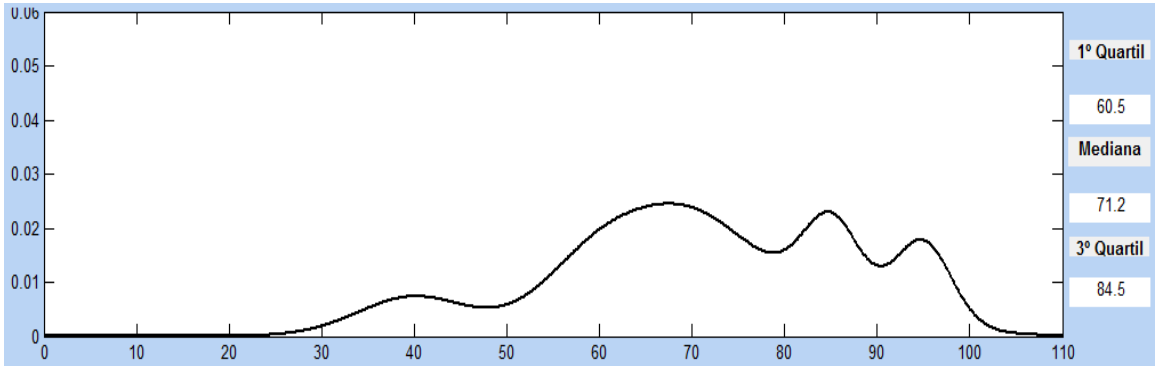


(b)

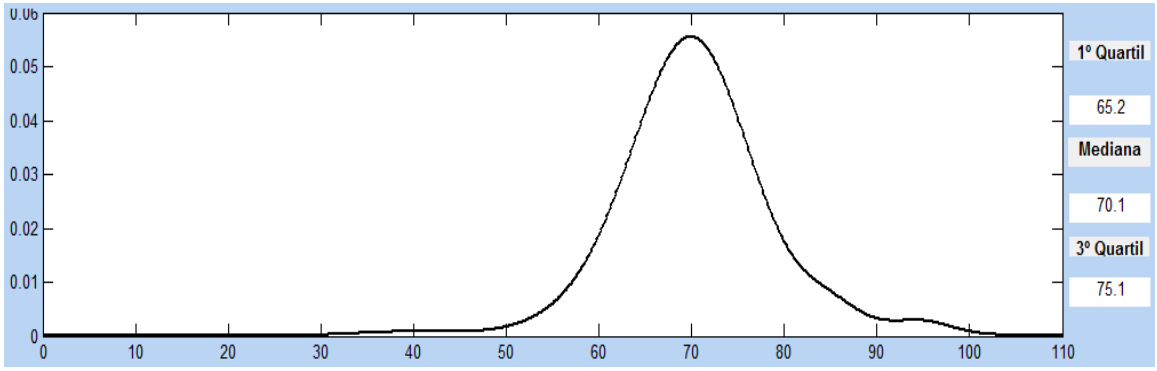


(c)

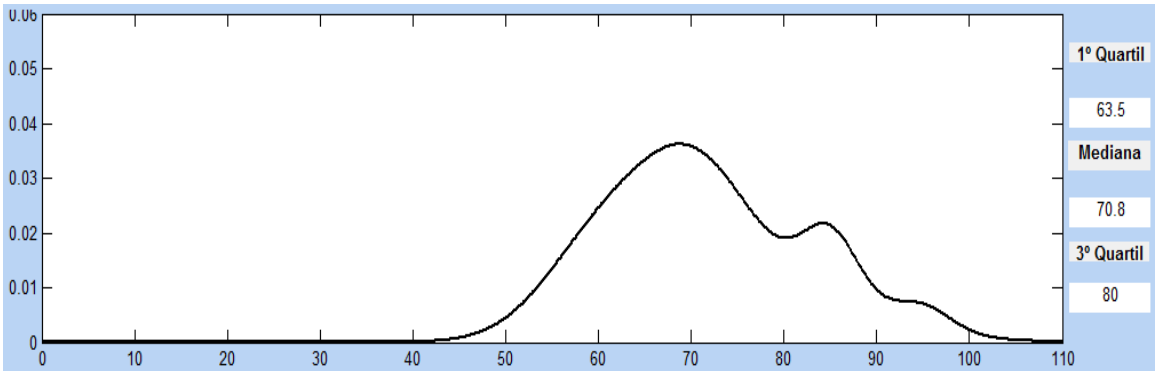
Figura 3.12 - Densidades geradas para o atributo Impacto Económico ao se atribuir pesos aos entrevistados: (a) Eq. 3.1; (b) Eq. 3.2; (c) Eq. 3.3



(a)



(b)



(c)

Figura 3.13 - Densidades geradas para o atributo Impacto Social ao se atribuir pesos aos entrevistados: (a) Eq. 3.1; (b) Eq. 3.2; (c) Eq. 3.3

Encerrada a 1ª ronda, concluímos pela necessidade de uma 2ª ronda de perguntas. Para esta ronda, decidimos apresentar como *feedback* aos analistas apenas os gráficos das densidades resultantes da aplicação da Eq. 3.2.

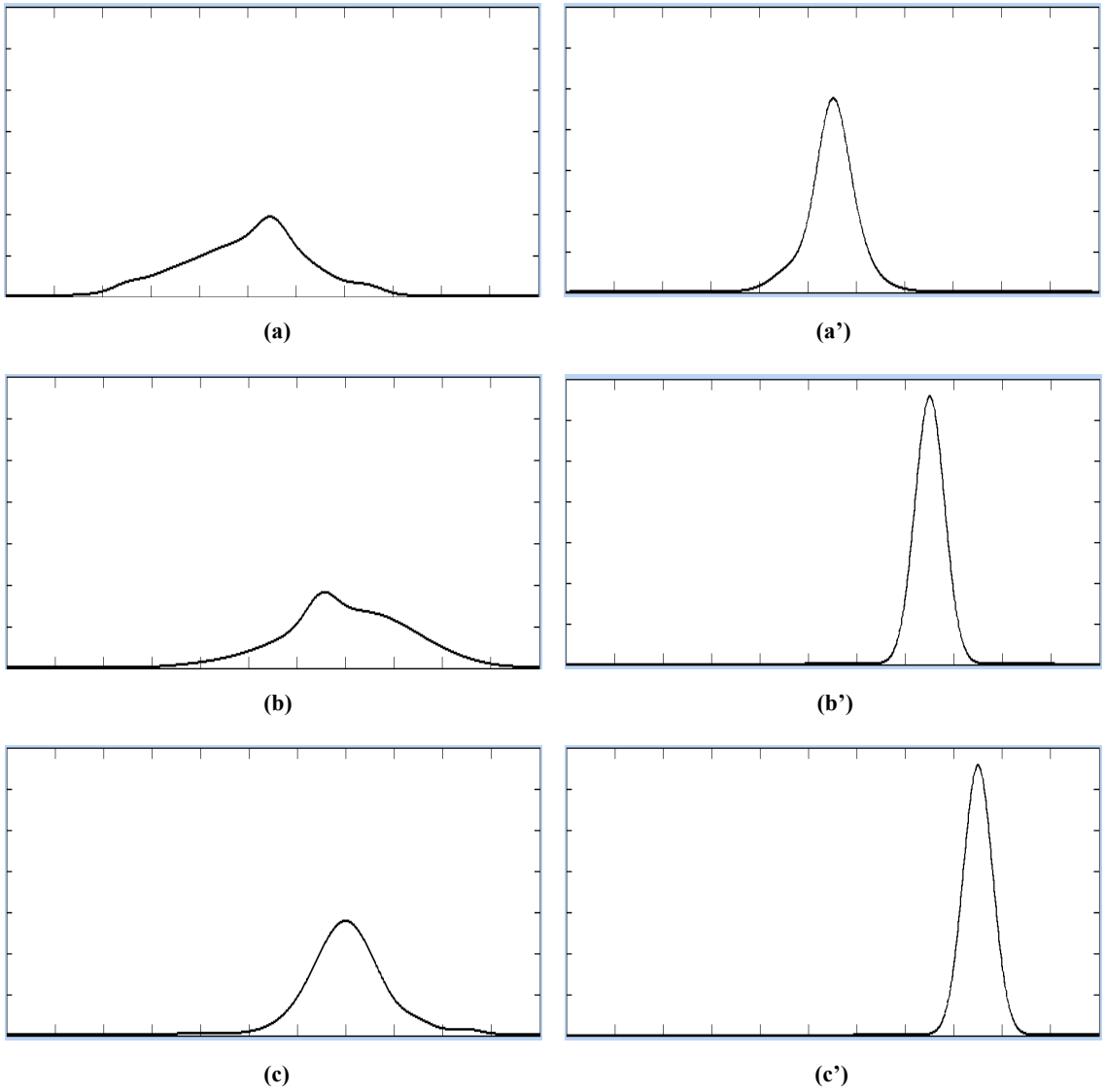


Figura 3.14 - Evolução das densidades estimadas, para os 3 atributos, da 1ª ronda (a,b,c) para a 2ª ronda (a',b',c')

A Figura 3.14 mostra a evolução das densidades geradas, da primeira para a segunda ronda de consultas. Os quadros (a-a'), (b-b') e (c-c') são referentes aos atributos Impacto Ambiental, Impacto Económico e Impacto Social, respetivamente.

Podemos observar que, para qualquer dos atributos, se obteve uma densidade unimodal, ou quase, e uma significativa redução da dispersão, pelo que se considerou ter sido alcançado suficiente consenso.

Note-se que, da primeira para a segunda ronda, os analistas optaram livremente por criar alguma distinção na preferência entre os atributos Impacto Económico e Impacto Social. Tendo em atenção as medianas das densidades na 2ª ronda — respetivamente: 55.1, 75 e 85 — pode-se concluir que, globalmente, o grupo preferiu atribuir maior importância

ao atributo Impacto Social e menor importância ao atributo Impacto Ambiental. Caso se pretenda dispor de um conjunto de pesos normalizados, com soma unitária, basta reescalar linearmente os valores das medianas registadas no fim do processo — respetivamente: 0.256, 0.349 e 0.395.

4 RISCO E DECISÕES

4.1 INTRODUÇÃO

A Análise de Risco e a Análise de Decisão cobrem uma série de conceitos, abordagens e ferramentas para a avaliação que, em muitos contextos, são complementares. Refira-se, entretanto, a confusão que pode resultar do uso da palavra **risco** em contextos e com propósitos muito diferentes: "decisão sob risco" (quando todas as variáveis exógenas são aleatórias), "aversão/propensão/neutralidade ao risco" (quando é dada especial atenção a consequências adversas das escolhas feitas), etc. Também não se deve confundir "redução do risco" com "redução da incerteza".

Numa primeira abordagem, a teoria económica apresenta a possibilidade de tomada de decisões num quadro de referência em que o risco e a incerteza não têm lugar. Num segundo momento, a hipótese de ausência de risco deve ser colocada de lado para que se possam enfrentar situações mais complexas, em que as decisões são tomadas em ambiente de risco e incerteza.

Muitas decisões de gestão estão sujeitas a incertezas significativas e o risco torna-se um fator primordial. Um bom exemplo é a alocação de recursos de defesa para a proteção de um porto, ora abordado, onde a quantidade de possíveis estados da natureza ou de possíveis rumos de ação dos atacantes e defensores é muito elevada. Até mesmo os custos e capacidades dos vários componentes que podem constituir o sistema de defesa, como, por exemplo, sensores e embarcações de patrulha, podem ser incertos. Portanto, uma boa decisão pode ser definida como aquela que, apesar de todas as incertezas, é tão racional quanto uma decisão tomada num ambiente com informação completa, onde são conhecidas todas as alternativas e suas consequências, avaliadas, em retrospectiva, pela diferença da recompensa dos resultados gerados (Cox, 2012). Estas circunstâncias, entre

muitas outras, levam a que as decisões para alocação de tais recursos possam ser consideradas como decisões de gestão de risco. Gestão do risco, como referido no Capítulo 1, é um processo subsequente à avaliação dos riscos, onde se torna possível otimizar as decisões por escolha de entre um conjunto de alternativas possíveis. A avaliação de riscos, que deve considerar o conhecimento obtido acerca da atitude do decisor perante o risco, deve fornecer recomendações robustas ao processo de decisão num contexto de gestão de riscos. Isto é, o comportamento de propensão, aversão ou neutralidade perante o risco expresso por cada agente de decisão afigura-se como absolutamente fundamental, uma vez que, sem ele, não poderemos avaliar o risco associado a cada potencial solução.

Em virtude dos motivos expostos, este capítulo está dividido, basicamente, em duas partes: a primeira, formada pelas Secções 4.2, 4.3 e 4.4, tem como objetivo fazer um enquadramento da terminologia que pode ser utilizada numa avaliação de riscos para apoiar um processo de decisão caracterizado por um ambiente de profunda incerteza e apresentar a teoria da utilidade e a sua extensão, multitatributo. Na segunda parte, nas Secções 4.5 e 4.6, é apresentada uma revisão dos métodos de agregação de funções de utilidade individuais e, em seguida, é feita uma proposta para a agregação de funções de utilidade individuais num contexto de decisão em grupo.

4.2 TERMINOLOGIA

Um problema de análise de decisão pode ser considerado relativamente simples se:

- Envolver apenas 1 estágio de decisão, e não múltiplos (em sequência);
- Os conjuntos de valores relevantes das variáveis endógenas (i.e., variáveis de decisão) e das variáveis exógenas têm cardinal relativamento pequeno, de forma a possibilitar uma avaliação exaustiva e em tempo útil.

As alternativas dizem respeito aos valores possíveis de apenas uma única variável de decisão ou de combinações possíveis de valores de 2 ou mais variáveis de decisão independentes — por exemplo, $X_1 =$ número de botes de patrulha; $X_2 =$ regime de patrulha; etc.

Nem sempre é prático enumerar e incluir na análise todas as possíveis alternativas, o que pode comprometer a validade das conclusões. Pode ser excluída da análise qualquer alternativa que, logo à partida, seja claramente dominada por outra,

nomeadamente, se for de qualidade inferior sob qualquer das condicionantes possíveis. Por outro lado, não é aconselhável ignorar aquilo que se pode designar por "opção zero", isto é, manter o *status quo* e não fazer nada — pode até acontecer que essa seja mesmo a melhor alternativa e, mesmo que não seja, a sua inclusão ajuda a calibrar a avaliação das restantes.

Relativamente às variáveis exógenas, podemos considerar dois tipos:

- **Variáveis aleatórias**: aquelas cuja incerteza, presente ou futura, é mais facilmente quantificável, probabilisticamente, com base na análise de dados históricos (por exemplo, Y_1 = temperatura da água do mar; Y_2 = correntes de maré);
- **Variáveis não aleatórias**: aquelas em que existe uma falta de conhecimento, sendo difíceis de quantificar com base em evidências factuais, passadas ou presentes. Não são conhecidas as probabilidades associadas, ou seja, o padrão de aleatoriedade não é conhecido. No entanto, há a conveniência em identificar quais delas são suficientemente plausíveis e preocupantes (por exemplo, Z_1 = comportamento de um terrorista; Z_2 = armamento usado num potencial ataque).

Como instrumento de adequação ao problema abordado neste trabalho, designamos por **variáveis adversariais** as variáveis exógenas não aleatórias; não se supõe o conhecimento de distribuições de probabilidade e duvida-se da fiabilidade de estimar subjetivamente tais distribuições.

Em análise de decisão, condições ou eventos futuros dependentes de um contexto incerto, considerados no problema decisório, são chamados **estados da natureza**. Por vezes, na literatura, os estados da natureza são designados como cenários, eventos, pressupostos, entre outros, o que se presta a confusões terminológicas. Por outro lado, com o objetivo de uniformizar as definições usadas neste trabalho, consideramos razoável usar a palavra ***setting*** para designar um qualquer estado da natureza. Os *settings* são, em geral, combinações **plausíveis** de **níveis** das variáveis exógenas (aleatórias ou adversariais) e dizem respeito a variáveis condicionantes da valoração das alternativas, isto é, num contexto de planeamento de recursos de defesa, são variáveis que definem possíveis contextos operacionais a serem executados num teatro de operações.

Neste momento, torna-se importante apresentarmos a distinção entre cenário e *setting* utilizada no planeamento de dispositivos de defesa, interpretada de *NATO Long-Term Defence Planning Handbook* (Bakken, 2003) e adaptada para este trabalho. A

definição de cenário estende o conceito de *setting* pela inclusão de eventuais elementos relacionados com a defesa, ou seja, das medidas de proteção a considerar. Logo, um ***setting*** refere-se ao contexto e condições de um **cenário** sem ainda considerar aqueles elementos de defesa. No problema aqui tratado, um *setting* é essencialmente definido pelas condições ambientais que podem influenciar as intenções e o comportamento de uma potencial ameaça (meteorologia, tráfego marítimo, correntes marítimas, etc.) e pelo tipo de ameaça propriamente dita (incluindo tática de ataque e armamento). A Figura 4.1 ilustra a diferença entre os conceitos.

Portanto, de forma resumida, devem ser enumerados os *settings*, resultantes de combinações plausíveis de valores das **variáveis exógenas** (adversariais ou aleatórias) relevantes, $\{\theta_j\}_{j=1,\ldots,n}$, bem como as alternativas, resultantes de combinações possíveis de valores das **variáveis endógenas (variáveis de decisão)** relevantes, $\{a_i\}_{i=1,\ldots,m}$.

Desta forma, designamos por **situação** (a_i, θ_j) a consequência de escolher a_i e "acontecer" — simultaneamente ou posteriormente — θ_j. Para cada (a_i, θ_j), é calculado o respetivo valor, $v_{ij} = Valor(a_i, \theta_j)$. A matriz ($m$ x n) contendo esses valores é designada por **tabela de decisão.**

Normalmente, o valor $v_{ij} = Valor(a_i, \theta_j)$ é um número, porém, pode acontecer que seja um intervalo, uma densidade de probabilidade, ou, até mesmo, pode ser definido por níveis qualitativos, não necessariamente convertidos em números — por exemplo, os desempenhos "muito mau", "mau", "razoável", "bom" e "muito bom".

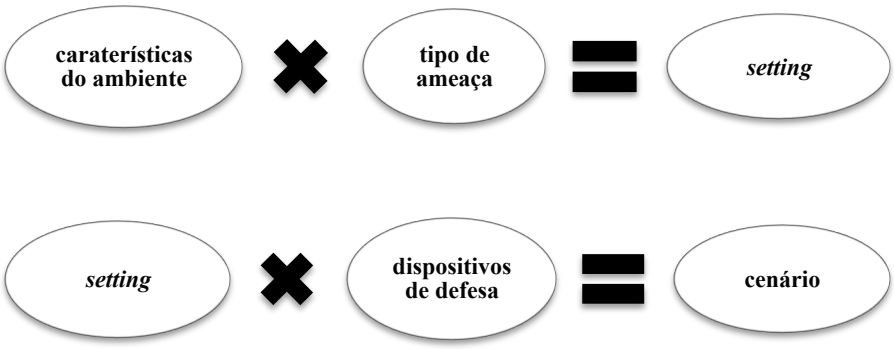


Figura 4.1 - Diferença entre *setting* e cenário

Independentemente do contexto do problema de decisão — seja em medicina, economia ou segurança, etc — esta avaliação pode resultar:

- de uma medição objetiva, por observação do mundo real; ou,
- de uma estimação por aplicação de um modelo analítico; ou,
- de uma estimação por aplicação de um programa de simulação; ou
- de uma estimação subjetiva.

Os valores são expressos em escalas de medidas. Existem basicamente quatro tipos de escalas (Stevens, 1946):

- Escala nominal: nível mais elementar de mensuração. Utiliza números ou nomes para identificação ou classificação. Não permite nenhuma operação aritmética. A sua principal função é a distinção entre os elementos;
- Escala ordinal: além da distinção entre elementos, é enriquecida com uma relação de ordem entre os mesmos;
- Escala intervalar: além de distinção e ordem, introduz uma regra de combinação entre elementos na forma de uma "distância";
- Escala de razão: a mais completa das escalas, onde é acrescentada à escala intervalar uma origem, de valor absoluto nulo.

Em todos os casos, pode ser aplicada uma função utilidade: $u_{ij} = Utilidade\left(v_{ij}\right)$. Uma função utilidade é uma função que associa um número real $u(x)$ para cada x no espaço de avaliação e será explicada com mais detalhes no decorrer deste capítulo. Desde já, podemos assinalar que, nesta abordagem, uma estimativa subjetiva poderá ou não ser logo elicitada como uma apreciação subjetiva (utilidade).

Uma **tabela de perda** consiste numa tabela de decisão preenchida com valores que representem malefícios (custos, perdas, desutilidades,…). Basta tomar os simétricos dos v_{ij} para converter o problema num de minimização, uma vez que $\min f(x) = -\max\left(-f(x)\right)$.

Tabela 4.1 - Tabela de perda, correspondente à avaliação de 4 alternativas face a 8 *settings*

			z_{11}				z_{12}				
			y_{11}		y_{12}		y_{11}		y_{12}		
			y_{21}	y_{22}	y_{21}	y_{22}	y_{21}	y_{22}	y_{21}	y_{22}	
			θ_1	θ_2	θ_3	θ_4	θ_5	θ_6	θ_7	θ_8	
x_{11}	x_{21}	a_1	v_{11}							v_{18}	V_1
	x_{22}	a_2									V_2
x_{12}	x_{21}	a_3									V_3
	x_{22}	a_4	v_{41}							v_{48}	V_4

A Tabela 4.1 mostra um exemplo de uma tabela de perda com todas as combinações de 4 alternativas versus 8 *settings*, totalizando 32 situações. No exemplo, todas as variáveis possuem dois níveis, ou seja:

Variáveis de decisão: X_1 (com níveis x_{11} e x_{12}) e X_2 (com níveis x_{21} e x_{22}).

Alternativas: $a_1 = \left(X_1 = x_{11}, X_2 = x_{21}\right)$, ..., $a_4 = \left(X_1 = x_{12}, X_2 = x_{22}\right)$.

Variáveis aleatórias: Y_1 (com níveis y_{11} e y_{12}) e Y_2 (com níveis y_{21} e y_{22}).

Variável adversarial: Z_1 (com níveis z_{11} e z_{12}).

Settings: $\theta_1 = \left(z_{11}, y_{11}, y_{21}\right)$, …, $\theta_8 = \left(z_{12}, y_{12}, y_{22}\right)$

Situações: $\left(x_{11}, x_{21}, z_{11}, y_{11}, y_{21}\right)$, …, $\left(x_{12}, x_{22}, z_{12}, y_{12}, y_{22}\right)$

Caso haja lugar para uma avaliação com múltiplos critérios e/ou múltiplos agentes de decisão, supõe-se que foram, entretanto, feitas agregações apropriadas, para a obtenção de valores escalares. Há inúmeros **operadores de agregação** possíveis, com diferentes propriedades teóricas. Os mais comuns são as medidas extremais (máximos / mínimos) e as médias (aritméticas ou geométricas, simples ou ponderadas). Portanto, pretende-se obter, para cada alternativa, um valor global V_i, por agregação dos valores $\left\{v_{ij}\right\}$. Depois, identifica-se qual a alternativa a escolher, a_{i^*}, tal que $V_{i^*} = \max\left\{V_i\right\}$.

Outra discussão diz respeito às condições a que está sujeita uma análise de decisão. São habitualmente identificados 3 tipos de problemas.

Decisão sob certeza: a certeza é um estado de conhecimento perfeito, em que o tomador de decisão tem informações completas sobre o problema decisório com o qual se defronta, o que lhe permite escolher a alternativa que, garantidamente, se comprovará *a posteriori* ser a melhor.

Decisão sob risco: decisão sob incerteza quantificada probabilisticamente. Supõe-se disponível conhecimento das distribuições de probabilidade associadas às variáveis exógenas. Neste caso, para escolher a melhor alternativa pode-se considerar, por exemplo, o critério max EMV (*expected monetary value*). No entanto, em vez de valor monetário esperado (lucro/custo), podemos ter o conceito análogo de utilidade, ou *desutilidade*, esperada.

Decisão sob incerteza estrita: decisão sob incerteza epistémica, em que todas as variáveis exógenas são adversariais, isto é, nada é conhecido sobre as suas probabilidades, abdicando-se de as estimar subjetivamente através do julgamento de especialistas com experiência no assunto. Especificamente, nas circunstâncias do problema aqui investigado, o decisor/especialista pode enumerar os possíveis *settings*, porém, é incapaz de formular probabilidades fiáveis sobre os mesmos. Nestes casos, a escolha a_{i^*} pode ser feita a partir de alguns critérios, entre eles (French, 1986): o critério de Laplace, o critério Maximax, o critério Maximin (ou de *Wald*), o critério de Hurwicz e o critério Minimax (de Savage).

Decisão sob incerteza parcial: embora isso seja relativamente pouco discutido na literatura, num problema podem coexistir variáveis exógenas de ambos os tipos, sobretudo em problemas de avaliação de riscos. Isto é, consideram-se simultaneamente variáveis exógenas para as quais se conhece a respetiva distribuição de probabilidade e variáveis exógenas cuja incerteza não é quantificada (probabilisticamente), ou seja, estamos perante problemas mistos. Para lidar com problemas deste tipo, pode-se tentar a conversão de variáveis adversariais em variáveis aleatórias, e assim uniformizar o tratamento das variáveis exógenas. Para isso, pode-se recorrer à elicitação e agregação das estimativas subjetivas de um painel de especialistas, por exemplo através do método Delphi Intervalar apresentado no Capítulo 3. Nesse caso, será suficiente estimar as probabilidades condicionais $P\left[Z_1 = z_{11} \middle| Y_1 = y_{11} \wedge Y_2 = y_{21} \right]$, etc. Aliás, em problemas relacionados com *safety risk* é habitual que variáveis aleatórias ambientais tenham influência em variáveis adversariais. Outra via possível consiste em, simplesmente, abdicar da informação sobre

probabilidades das variáveis aleatórias, e tratá-las como se fossem não aleatórias, reduzindo o problema a um de decisão sob incerteza estrita.

4.3 TEORIA DA UTILIDADE

Historicamente, é atribuído a Bernoulli (1738) o crédito de ter sido o primeiro a apresentar o conceito de *utilidade*, ao argumentar que a determinação do valor de um item não pode ser baseada no seu preço, mas sim na utilidade que ele fornece. A Teoria da Utilidade permite avaliar as consequências das escolhas num problema de decisão por meio de um processo de elicitação que procura incorporar as preferências do decisor e o seu comportamento em relação ao risco. Isto significa que as preferências entre as consequências podem ser expressas através de uma função real, chamada *utilidade*. Com esta abordagem, as avaliações subjetivas feitas pelos agentes de decisão passaram a ter um papel fundamental, o que permitiu um avanço significativo no estudo de problemas de avaliação e análise de risco.

Todavia, a escolha sob incerteza parecia às vezes algo enigmático que não se adaptava adequadamente à teoria da Utilidade. Esta situação foi alterada, particularmente, em meados do século XX, a partir dos trabalhos de Von Neumann e Morgenstern (1947) e de Savage (1954), que apresentaram as bases axiomáticas de como um indivíduo considerado racional deveria se comportar perante o risco ou a incerteza. Se o decisor aceita esses axiomas pode-se considerar que ele é coerente nas suas preferências e, desta forma, as inconsistências na estruturação do problema são evitadas.

Os axiomas preveem que os decisores possam estabelecer uma relação de preferências ($\succ$, "mais preferível do que"; $\prec$, "menos preferível do que"; ou, $\sim$, "indiferente a") e que sejam capazes de declarar as suas escolhas em relação a uma *lotaria* entre os valores das consequências. Lotarias são, tipicamente, jogos que conferem ganhos x com probabilidade p e ganhos y com probabilidade $1-p$, sendo representados por $\left[x, p;\ y, 1-p\right]$ ou, mais simplesmente, por $\left[x, p, y\right]$.

De entre os axiomas mais comummente encontrados na literatura, referimos:

— Axioma da ordenabilidade: dadas as consequências x_1 e x_2, podemos dizer que $x_1 \succ x_2$ ou $x_1 \sim x_2$ ou $x_1 \prec x_2$. Ou seja, perante duas alternativas, o

decisor deve preferir uma delas ou então classificar as duas como igualmente preferíveis;

— Axioma da transitividade: dadas três consequências, x_1, x_2 e x_3, se $x_1 \succ x_2$ e $x_2 \succ x_3$, então $x_1 \succ x_3$. Se $x_1 \sim x_2$ e $x_2 \sim x_3$, então $x_1 \sim x_3$;

— Axioma da continuidade: dados três valores x_1, x_2 e x_3, se $x_1 \succ x_2 \succ x_3$, então existe p, $0 < p < 1$, tal que $x_2 \sim [x_1, p;\ x_3, 1-p]$;

— Axioma da substituição ou da independência de preferências: se $x_1 \sim x_2$, então $[x_1, p;\ x_3, 1-p] \sim [x_2, p;\ x_3, 1-p]$;

— Axioma da monotocidade: se $x_1 \succ x_2$, então $[x_1, p;\ x_2, 1-p] \succ [x_1, q;\ x_2, 1-p]$ se e somente se $p > q$ $\left(0 < p < 1 \text{ e } 0 < q < 1\right)$.

Segundo a teoria, para um dado conjunto de situações, são associados valores numéricos que expressam utilidades, devendo ser escolhida a alternativa que maximizar a utilidade esperada. Essas consequências estão associadas a lotarias, mesmo que os resultados não sejam provenientes de experiências aleatórias. O princípio da utilidade esperada permite valorar a distribuição de probabilidades dos possíveis resultados de uma decisão e, portanto, estabelecer relações de preferência global entre alternativas.

De forma geral, uma função de utilidade deve ser definida para medir a utilidade dos tomadores de decisão em todo o espaço das consequências possíveis, em vez de mensurar apenas um valor. Contudo, existe certo paralelismo entre o conceito de funções de utilidade e o de funções de valor. De facto, qualquer modelo baseado na utilidade substantiva de um sujeito reflete, antes de mais, a sua hierarquização de valores. Assim, um modelo de utilidade pode ser encarado como a formalização de um conceito de modelo de valor mais abrangente. Serão, sobretudo, usados em problemas em que existem diferentes *settings*, aos quais se associam diferentes probabilidades, enquanto as funções de valor devem ser usadas em situações onde as consequências são certas (Sarabando, 2010).

Uma função de utilidade apenas coincide com a função de valor se o decisor for indiferente perante o risco. No entanto, Winterfeldt e Edwards (1986) consideram que a distinção na prática entre função de valor e função de utilidade é questionável. Nesta mesma discussão, Keeney e Raiffa (1976) e Belton e Stewart (2002) referem-se a uma função de representação de preferências sob certeza como "função de valor" e a uma função de representação sob risco como "função de utilidade". Como assinalado por Dias

(2000), os motivos estão relacionados com o facto de que "uma consequência sem risco é na realidade o valor que se atribui à utilização (que envolve incerteza) dessa consequência; a aversão ao risco pode ser modelada por funções de valor côncavas ou pela presença de critérios específicos; as escolhas repetitivas tendem a eliminar a aversão ao risco; e, sobretudo, os erros de modelação, quer no caso da função de valor, quer no caso da função de utilidade, são mais significativos do que a subtil distinção entre utilidade e valor".

Especificamente, uma função de utilidade é normalmente construída tal que os atributos com as maiores utilidades esperadas são preferidos àqueles com baixas utilidades esperadas. Todavia, no problema em questão, que visa a redução do risco de segurança, este risco é quantificado com base em funções de **desutilidade**, uma vez que são preferíveis os menores resultados, definidos numa escala entre 0 e 1, onde 1 é o pior resultado plausível de um atributo.

Em problemas de decisão em condições sob risco, a função de utilidade é, normalmente, obtida a partir de questionários feitos ao decisor, com vista a elicitar as suas preferências para lotarias válidas no domínio das consequências de um atributo. Assim, um processo de elicitação consiste na avaliação da seguinte expressão:

$$\left[x, p, y\right] \Re \left[w, q, z\right]$$

onde um parâmetro é desconhecido e todos os outros são dados. Cabe ao decisor especificar o valor do parâmetro desconhecido para o qual uma das relações $\Re$ ($\succ$, $\prec$ ou ~) seja satisfeita.

Segundo Jiménez *et al*. (2003), os valores de utilidade podem ser avaliados usando três diferentes métodos, a seguir resumidos, e que são dependentes do conhecimento e das características dos atributos sob consideração.

O Método Direto é de fácil implementação e a elicitação da função de utilidade, como o próprio nome diz, é direta, $U\left(x_i\right) = p_i$. Compete ao decisor quantificar as diferenças dos valores das consequências de cada atributo dentro de uma escala intervalar. Geralmente, os valores extremos são quantificados como 0 e 1, ou seja, os menos preferidos e os mais preferidos, respetivamente, sendo os valores intermédios elicitados diretamente pelo decisor.

O método do Equivalente Certo consiste num conjunto de instruções para a construção das curvas das funções de utilidade. As instruções pressupõem que as consequências das alternativas tenham sido avaliadas segundo cada atributo. O procedimento básico do método começa por identificar quais as quantidades mais

preferidas, $x_{\max}$, e as menos preferidas, $x_{\min}$, de entre as consequências possíveis do atributo avaliado. Todos os outros níveis de consequências, x, estão entre esses valores $\left(x_{\max} \succ x \succ x_{\min}\right)$. As utilidades dos valores extremos são as primeiras a serem avaliadas, a fim de definir a escala de medição. Geralmente, $u\left(x_{\min}\right)=0$ e $u\left(x_{\max}\right)=1$. Posteriormente, é necessário que seja especificado um valor, x^*, dentro do intervalo $\left[x_{\min}, x_{\max}\right]$, denominado Equivalente Certo ($EC(p)$), para o qual $x^* \sim \left[x_{\max}, p, x_{\min}\right]$, ou seja:

$$u\left(x^*\right) = p\,u\left(x_{\max}\right) + (1-p)\,u\left(x_{\min}\right)$$

Segundo Winterfeldt e Edwards (1986), o Método do Equivalente Certo é frequentemente empregue de acordo com os seguintes passos e que envolvem a bissecção do intervalo de valores:

- Definição do conjunto $X = \left\{x_{\min}, ..., x_i, ..., x_{\max}\right\}$, dos valores das consequências possíveis de um atributo;
- Seleção dos valores de X mais e menos preferidos: $x_{\max}$ e $x_{\min}$;
- Definição do nível $EC(0.5)$, em que o decisor é indiferente à lotaria $\left[x_{\max}, 0.5, x_{\min}\right]$;
- Definição dos demais pontos para a construção da curva, nomeadamente através das relações de indiferença $EC\left(0.25\right) \sim \left[EC\left(0.5\right), 0.5, x_{\min}\right]$ e $EC\left(0.75\right) \sim \left[EC\left(0.25\right), 0.5, x_{\min}\right]$.

O método da Probabilidade Equivalente é algo similar ao do Equivalente Certo. Nas lotarias do método do Equivalente Certo, é fixada a probabilidade p, e é pedido ao decisor que expresse os valores que acredita serem equivalentes às lotarias. No método da Probabilidade Equivalente, os valores são fixados e o decisor define a probabilidade *p* que satisfaz $\left[x_{\max}, p, x_{\min}\right] \sim x^*$. Em geral, escolhem-se como elementos de referência os valores que representam a pior consequência e a melhor consequência em *X*. O problema então é elicitar um conjunto de valores $x_i \in X$ tais que $x_{\min} \prec x_1 \prec ... \prec x_i \prec ... \prec x_n \prec x_{\max}$ utilizando-se uma das seguintes variantes do método:

— **Valores extremos**: $\left[x_{\min}, p_i, x_{\max}\right] \sim x_i$. Este método usa os pontos de referência do conjunto *X* em todas as elicitações. Se $u(x_{\min}) \equiv 0$ e $u(x_{\max}) \equiv 1$, então a probabilidade elicitada p_i é também a utilidade de x_i:

$$\begin{aligned} u(x_i) &= u\left(\left[x_{\min}, p_i, x_{\max}\right]\right) \\ &= p_i u(x_{\min}) + (1-p_i) u(x_{\max}) \\ &= p_i \end{aligned}$$

— **Valores adjacentes:** $\left[x_{i+1}, p_i, x_{i-1}\right] \sim x_i$. Ao invés de utilizar valores extremos, este método requer do decisor uma indiferença meramente local. Cada resposta do decisor implica uma equação da forma:

$$u(x_i) = p_i u(x_{i+1}) + (1-p_i) u(x_{i-1})$$

Daqui resulta um sistema de *n* equações algébricas lineares.

Embora muitos indivíduos achem difícil fazer afirmações sobre probabilidades, estão disponíveis protocolos e processos de treino para facilitar o processo de elicitação. Uma vantagem deste último método é que o decisor não precisa responder a questões para as quais a probabilidade ficaria naturalmente próxima de 0 ou de 1, tornando esse processo de elicitação menos sensível à falta de precisão das probabilidades especificadas pelo decisor (Farquhar, 1984).

4.3.1 COMPORTAMENTO QUANTO AO RISCO

A teoria da utilidade esperada explica as diferentes atitudes perante o risco e os seus axiomas permitem a construção de uma função de utilidade, a qual será de grande interesse para compreender os comportamentos das pessoas. Por outro lado, segundo Keeney e Raiffa (1976), esses comportamentos têm implicação direta na forma da função de utilidade:

— O decisor demonstra *propensão ao risco* se, e só se, a função de utilidade é convexa — isto é, se, para quaisquer $x_i, x_j \in X$ e $p \in \left[0,1\right]$,

$$p u(x_i) + (1-p) u(x_j) > u\left(p x_i + (1-p) x_j\right);$$

— demonstra *aversão ao risco* se, e só se, a função de utilidade é côncava:

$$p u(x_i) + (1-p) u(x_j) < u\left(p x_i + (1-p) x_j\right);$$

— demonstra *neutralidade ao risco* se, e só se, a função de utilidade é linear:

$$p u(x_i) + (1-p) u(x_j) = u\left(p x_i + (1-p) x_j\right).$$

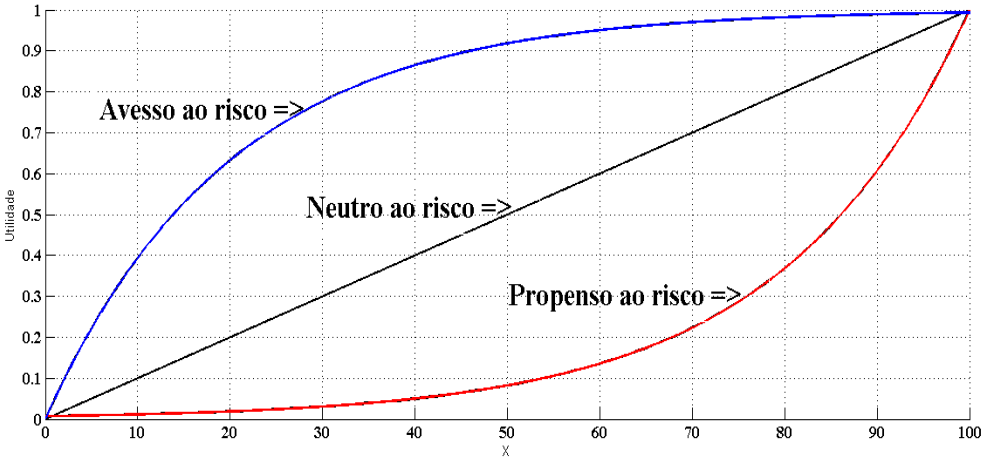


Figura 4.2 - Curvas que representam o comportamento do decisor perante o risco

As curvas de comportamento perante o risco são ilustradas na Figura 4.2. Podemos observar que uma atitude de aversão ao risco define utilidades mais elevadas para os valores relativos das consequências, quando comparado com uma atitude de propensão e neutralidade ao risco, enquanto uma atitude de propensão ao risco define as menores utilidades.

No contexto deste trabalho, assumiremos que os decisores expressam uma atitude de aversão ao risco constante. Para este caso, uma função frequentemente utilizada é a função de utilidade exponencial (Keeney e Raiffa, 1976), com a forma

$$u(x) = -e^{-rx},\ r > 0,$$

onde r designa o *parâmetro de aversão ao risco* — e o seu inverso, $R = 1/r$, é correspondentemente conhecido por *parâmetro de tolerância ao risco* — e x indica os possíveis valores das consequências. Esta fórmula define uma função exponencial amortecida negativa. No entanto, estabelecemos que as desutilidades devem ter valores positivos e serão então dadas pela seguinte função:

$$u(x) = 1 - e^{-rx},\ r > 0 \qquad \textbf{(4.1)}$$

A constante r é um valor abstrato que serve para quantificar o quão indesejável é o risco para uma determinada pessoa. É flagrante o elevado grau de subjetividade envolvido na definição desta constante e consequentemente da função de utilidade, problema que no contexto desta tese pode ser agravado. O valor deste parâmetro é absolutamente específico para determinada pessoa, face a determinado atributo, não devendo ser extrapolado para outro decisor ou outro atributo.

A escolha do valor de *r* pode ser feita por recurso a questionários de elicitação com base nos métodos já discutidos na subsecção anterior. Todavia, estes métodos dependem de estimativas pontuais e precisas para os diferentes dados de entrada, as quais podem ser fontes de inconsistências durante o processo de elicitação, pelo que têm sido propostas abordagens mais práticas e que exijam menos precisão por parte dos decisores (Jiménez *et al*., 2003). Algumas dessas propostas são baseadas em ferramentas visuais e na definição de intervalos, conforme a metodologia apresentada no Capítulo 3. Acompanhando esta linha de raciocínio, fazemos uma simples sugestão para a elicitação da curva de desutilidade exponencial da Eq. 4.1. O objetivo é proporcionar ao decisor a visualização de diversas curvas, para diversos parâmetros de aversão ao risco, escolhidos ou manipulados através de um *slider*. Para isto, foi desenvolvido um projeto de interface gráfica em ambiente MATLAB, ilustrado na Figura 4.3.

A interface pode ser utilizada no contexto da problemática abordada nesta tese. Primeiro, é necessário elicitar dos especialistas quais os intervalos das consequências de um ataque bem sucedido, em função de cada *setting*. Sugere-se que essas estimativas sejam feitas pelo método Delphi Intervalar. Em seguida, cada decisor deve definir um intervalo de valores do parâmetro *r*. Pelo manuseio do *slider*, cada decisor pode fazer uma análise de sensibilidade visual das curvas de desutilidade correspondentes.

Esta nossa proposta pode ser interpretada como uma variação, mais elaborada, do Método Direto de elicitação das curvas, onde o valor da variável *EC,* disponibilizado na interface, representa x_i : $u(x_i) = 0.5$.

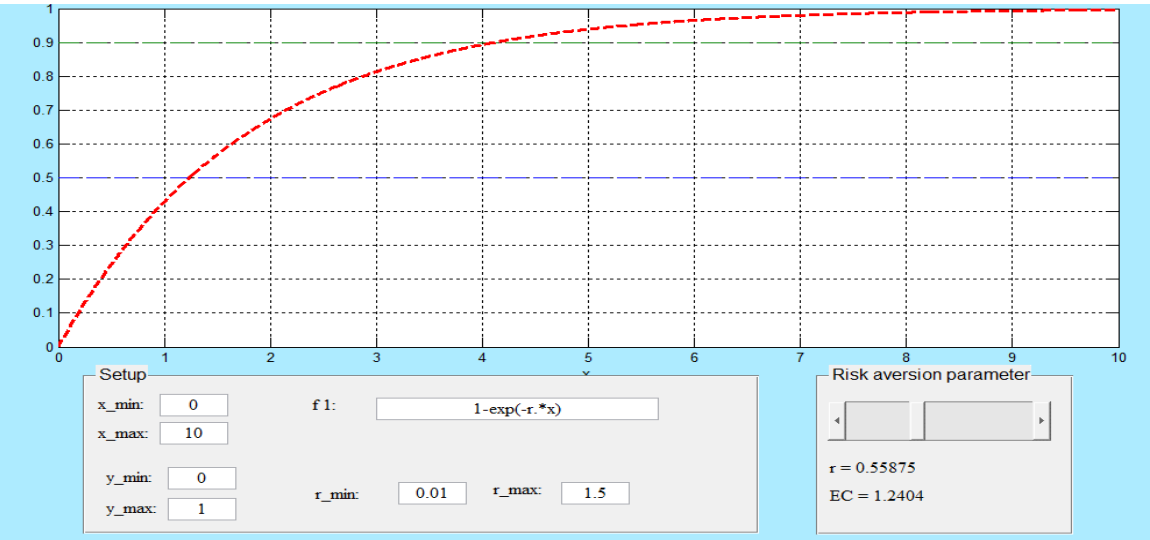


Figura 4.3 - Interface para elicitação das curvas de desutilidade

O Método Direto pode ser criticado devido à falta de uma boa justificação matemática (Wakker e Deneffe, 1996). Contudo, é um método simples e de fácil entendimento que pode ser adequado para um contexto onde a definição de lotarias, necessária para métodos mais elaborados do ponto de vista teórico, pode ser uma tarefa de difícil concretização.

Além disso, baseamo-nos no facto de que as decisões devem ser fundamentadas nos valores dos decisores, pelo que estes devem ser colocados no centro de todo o processo de pensamento estratégico que conduzirá, depois, à escolha de soluções. Podemos identificar os nossos valores, pensando no que queremos encontrar e no que queremos ter (Keeney, 2009).

4.4 TEORIA DA UTILIDADE MULTIATRIBUTO (MAUT)

O objetivo desta secção é apresentar resumidamente a Teoria da Utilidade Multiatributo (*Multiattribute Utility Theory* - MAUT), que será usada para a definição do índice de Criticidade no capítulo seguinte. Diversos exemplos de aplicação de MAUT no contexto da avaliação de riscos são disponibilizados na literatura, como: Hämäläinen *et al.* (2000), Wang e Bier (2011), Weil e Apostolakis (2001), Leung *et al*. (2004), Apostolakis e Lemon (2005), Rosoff (2009), Dillon *et al.* (2009), Butler *et al*. (2011) e Keeney e Winterfeldt (2011).

Keeney e Raiffa (1976) estenderam os conceitos da teoria da utilidade para o auxílio a problemas decisórios, nos quais cada alternativa pudesse ser descrita por uma lista de atributos. Os autores propuseram a construção de uma função matemática, capaz de agregar as informações dos múltiplos atributos de forma que, a cada alternativa, pudesse ser associada uma medida de utilidade. Isto torna possível elaborar ordens de preferências entre as alternativas. A teoria considera que, para cada um dos atributos, existe uma função de utilidade específica; posteriormente, quando agregadas, essas funções dão origem a uma função de utilidade multiatributo.

Para selecionar uma alternativa, *a*, de entre m possíveis, consideram-se vários atributos, $x_1, x_2, ..., x_n$. Os atributos representam consequências diretas no julgamento de uma alternativa e são medidos normalmente em unidades diferentes.

Como mencionado, torna-se necessário agregar as diferentes funções de utilidade de cada atributo. O modelo aditivo é, sem dúvida, o mais utilizado para agregar

preferências em problemas multiatributo. Com esta agregação, o modelo permite, com uma grande simplicidade e facilidade, fazer a ordenação das alternativas do problema em estudo, e é expresso da seguinte forma:

$$u(a_i) = \sum_{j=1}^{n} w_j \, u_j(a_i)$$

onde os $w_j \in [0,1]$ são pesos normalizados $\left(\sum_{j=1,\ldots,n} w_j = 1\right)$ e $u_j(a_i) \in [0,1]$ é a utilidade, segundo o *j*-ésimo atributo ($j = 1,\ldots,n$), para a alternativa a_i ($i = 1,\ldots,m$).

Contudo, conforme Keeney e Raiffa (1976), esta forma simples de agregação só é válida se for verificada a condição de independência mútua de preferências entre os atributos. Os atributos são mutuamente independentes se qualquer subconjunto desses atributos é preferencialmente independente do seu conjunto complementar. Esta questão é discutida, por exemplo, por Goodwin e Wright (1998).

Além disso, a forma aditiva não permite contemplar certas situações em que seria desejável que uma quantidade de um atributo dependa de uma quantidade de outro atributo.

Na literatura dedicada à análise multiatributo encontramos diversos exemplos de técnicas de agregação, como, por exemplo, a multiplicativa, que requerem condições de independência mais fracas (Keeney e Raiffa, 1976; Goodwin e Wright, 1998). Porém, na prática, a agregação aditiva possui uma grande facilidade de aplicação, tanto para o decisor como para o eventual analista. Keeney (2002) argumenta que a não verificação das condições de independência que permitem uma agregação simples é frequentemente fruto de uma estruturação deficiente. Edwards *et al*. (1988) e Stewart (1995) assinalam que a aproximação de um modelo multiplicativo por um aditivo é geralmente boa. Desta forma, sugerimos que uma função de utilidade aditiva é uma aproximação razoável com base nos elementos do problema tratado neste trabalho.

A agregação das componentes de um modelo de utilidade é feita após a atribuição de pesos a cada atributo, também designados na literatura como coeficientes de escala, constantes de escala ou ponderações. O peso de um atributo representa a importância relativa de mudar o nível de desempenho no atributo respectivo do seu pior nível (nível com valor igual a 0) para o seu melhor nível (nível com valor igual a 1), especificado pela decisão em consideração, comparado com o aumento do nível 0 para nível 1 no desempenho noutro atributo (Sarabando, 2010). Isto significa que a importância entre os critérios depende da compensação entre os mesmos. Portanto, não representam apenas a

importância relativa entre os atributos, sendo este um dos mais comuns erros cometidos (Keeney, 2002). Os pesos devem ser atribuídos cuidadosamente para assegurar que os resultados da avaliação sejam consistentes com as preferências do decisor e constituem habitualmente os parâmetros mais difíceis de obter. Existem diversas técnicas para elicitar os pesos, as mais comuns podem ser visualizadas na Tabela 4.2. Todavia, a elicitação de pesos é uma tarefa cognitiva, sujeita a diferentes vieses de comportamento (Belton, 2002), além dos valores elicitados variarem fortemente em função da técnica escolhida (Hämäläinen *et al*., 2001). As técnicas disponíveis na literatura, na prática, são determinadas pelos aspetos procedimentais de elicitação das preferências dos decisores. Portanto, sob o nosso ponto de vista, métodos com componentes que permitam a extração de tais preferências de uma forma relativamente mais interactiva podem ser mais úteis em contextos decisórios complicados. Um exemplo é apresentado por White e Holloway (2008): os autores fazem uma proposta com o objetivo de orientar um facilitador a colocar questões ao decisor de forma a obter respostas a respeito da alternativa mais preferível, de maneira que consuma menor tempo, esforços e expectativas e determine o melhor momento para interromper os questionamentos.

Tabela 4.2 - Métodos para definição de pesos

Métodos	Procedimento de avaliação
Direct Rating	Os pesos são atribuídos diretamente aos atributos, por exemplo, usando-se uma escala de 0 a 100.
Tradeoff Weighting	O decisor compara duas alternativas que se diferenciam por apenas dois atributos com os outros atributos mantidos fixos. Um dos atributos é ajustado até que as alternativas se tornem igualmente preferidas.
Alocação de Pontos	São distribuídos 100 pontos entre os critérios.
Swing Weighting	O decisor deve imaginar uma alternativa hipotética com as piores consequências. O decisor atribui 100 pontos ao atributo que ele escolheria para mudar do pior nível para o melhor nível. Em seguida, o decisor avalia as alternativas restantes e novamente escolhe a que considera melhor, atribuindo-lhe um valor inferior a 100 pontos. O processo continua até que todas as alternativas tenham sido pontuadas.
UTA	O tomador de decisão deve ordenar por ordem de preferência um pequeno subconjunto de alternativas, de forma global, sem as decompor critério a critério. Após a resolução de um problema de programação linear, o método determina o conjunto dos coeficientes de ponderação (pesos).
Rank-Order	Os critérios são classificados de acordo com as suas ordens de importância.

4.5 AGREGAÇÃO DE FUNÇÕES DE UTILIDADE NUM GRUPO

Em situações de decisão com múltiplas partes interessadas (*stakeholders*), é frequente que existam divergências de preferências entre eles e, mesmo que os valores dos parâmetros das curvas de aversão ao risco possam ser obtidos, não é claro como as preferências de múltiplos decisores podem ser combinadas.

Vários procedimentos têm sido sugeridos para a agregação das funções de utilidade. Segundo Bose *et al.* (1997), a agregação de preferências individuais numa função utilidade de todo o grupo — ou seja, uma relação matemática combinando as preferências individuais ou utilidades — tem sido estudada por investigadores desde o século XVIII. De entre os principais métodos podemos destacar: o princípio maximin; a regra da maioria; processos de negociação; regras de negociação; e as chamadas funções de bem-estar social (*Social Welfare Functions*) (Pattanaik, 2008). A definição de bem-estar social é baseada em conceitos da Teoria da Escolha Social (Myerson, 1996), teoria que tem fundamento no facto de que as decisões tomadas por grupos de indivíduos diferem fundamentalmente das decisões tomadas por um único indivíduo.

Uma função de bem-estar social é qualquer forma de agregação que garante que a função de utilidade da sociedade, ou seja, do grupo de indivíduos, é monotonicamente crescente na utilidade de cada indivíduo. A agregação pode ser definida por uma das seguintes formas, entre outras:

- Soma ou média das utilidades individuais, conhecidas como *classical utilitarian welfare functions*;
- Regra minimax, intitulada *Rawlsian welfare function*; nesta, o bem-estar de uma sociedade depende unicamente da pior avaliação individual feita no grupo;
- A função conhecida como *Bernoulli-Nash (average) social welfare function*, onde a utilidade final é alcançada pela média geométrica das utilidades individuais.

Ainda tendo como base conceitos da Teoria da Escolha Social, Arrow (1951) e Keeney (1976) investigaram a possibilidade de agregação das utilidades individuais a partir de funções ordinais (Arrow) e cardinais (Keeney) de forma a satisfazer, entre outras, a condição de *nondictatorship* — expressão que indica que nenhum indivíduo pode ditar a vontade social. Dias e Sarabando (2012) reinterpretam essa condição e propõem novas

formulações de modo a limitar a máxima influência que um indivíduo poderia ter sobre um grupo.

Outras formas de agregação são baseadas na caracterização de pesos que refletem a importância relativa dos membros do grupo. Uma delas é a apresentada por Keeney e Kirkwood (1975), onde a agregação é feita usando uma soma ponderada das utilidades esperadas de cada membro do grupo. Esta linha de raciocínio é seguida por alguns autores, entre os quais, Nakayama *et al.* (1979) e Salo (1995). Recentemente, Keeney (2013) apresenta um modelo baseado na comparação interpessoal e na importância relativa ou poder de cada membro do grupo para especificação de pesos. No entanto, segundo Sarabando (2010), a definição de pesos é uma tarefa difícil, que "requer comparações relativas à autoridade, experiência e especialidade dos elementos do grupo".

Em todos estes casos, a operação de agregação é definida sobre as curvas de utilidade, mas há também propostas para procedimentos de agregação que podem ser definidos simplesmente pela agregação dos parâmetros individuais de comportamento perante o risco, $\{r_i\}_{i=1,\ldots,m}$. Um exemplo simples, que considera a agregação dos valores individuais do parâmetro de aversão ao risco, é apresentado por Bordley e Licalzi (2000). Concretamente, consideram a agregação de funções de utilidade exponenciais, $u_i(x) = 1 - e^{-r_i x}$, da seguinte forma:

$$u_g(x) = 1 - \prod_{i=1}^{m} \left(1 - u_i(x)\right)$$

daí resulta que

$$u_g(x) = 1 - e^{-\left(\sum_{i=1}^{m} r_i\right)x}$$

Nesse caso, e dado que $\sum_i r_i > \max_i r_i$, o grupo exibiria uma aversão ao risco superior à de qualquer dos indivíduos. Os autores argumentam sobre a razoabilidade desta propriedade à luz do **efeito de polarização** observado empiricamente por Doise (1969), segundo o qual a opinião final de um grupo, após discussão, é mais extrema do que a **média** das opiniões individuais iniciais. Contudo, caso n = 10 indivíduos demonstrassem exatamente o mesmo grau de aversão ao risco — por exemplo, $r_i = 0.2$ —, o grupo, em conjunto, teria então uma aversão ao risco manifestamente exagerada, $\sum r_i = 2$. Para efeito de comparação, ilustramos essas duas curvas de aversão ao risco na Figura 4.4.

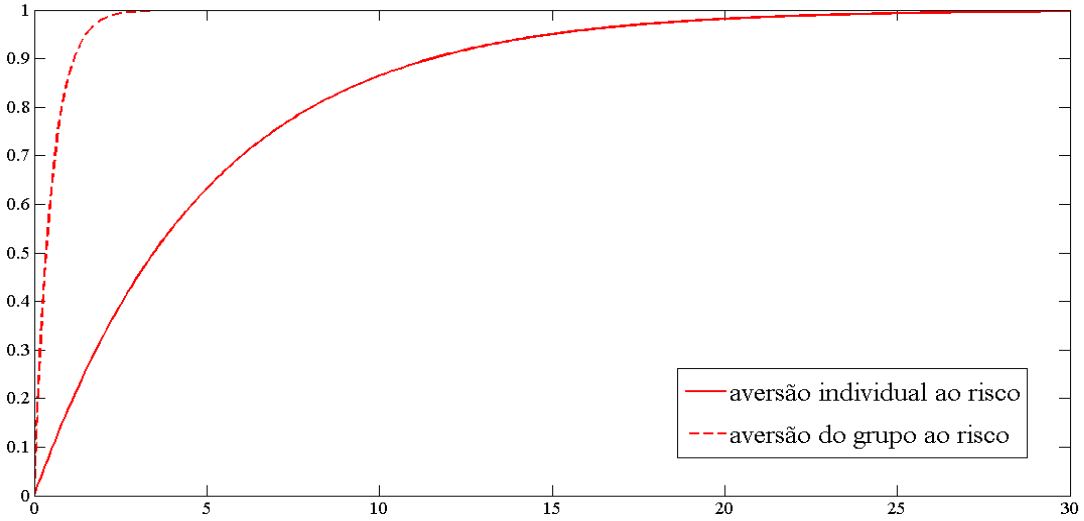


Figura 4.4 - Curvas de aversão individual e do grupo ao risco

Moscovici *et al.* (1972) observam que, nos processos de decisão em grupo, a mudança para posições mais extremadas está diretamente correlacionada com o grau de interação e discussão dentro do grupo. Pelo contrário, o método Delphi, ao preservar o anonimato, e ao limitar a interação dos indivíduos apenas com o coordenador, reduz de forma natural a possibilidade de ocorrência desse efeito de polarização. No caso particular de existir, à partida, consenso perfeito entre os indivíduos, não é razoável concluir que a opinião representativa do grupo deva ser diferente dessa posição comum, muito menos que seja consideravelmente diferente.

4.6 NOVA PROPOSTA PARA AGREGAÇÃO DE FUNÇÕES DE UTILIDADE NUM GRUPO

No problema que investigamos, desejamos seguir a linha de raciocínio apresentada no Método Delphi Intervalar: a possibilidade de elicitar as preferências individuais de cada agente de decisão sem a interação dos demais membros do grupo, evitando, desta forma a sua influência. A agregação de curvas de utilidade individuais deve, então, ser feita numa fase posterior, de forma automatizada e que permita a visualização da curva gerada para o grupo.

Assim, apresentamos uma proposta para a agregação das funções de utilidade de um grupo por meio da média geométrica dos parâmetros individuais de comportamento perante o risco, $\{r_i\}_{i=1,\ldots,m}$, associados às funções de utilidade individuais (isto é, de cada

membro do grupo). Explicitamente, a função de utilidade do grupo, $u^*(x)$, será definida por:

$$u^*(x) = 1 - e^{-r^* x}$$

onde

$$r^* = \left(\prod_{i=1}^{m} r_i \right)^{1/m}$$

Esta proposta obedece à regra básica de uma *social welfare function* — a função do grupo deve ser monotonicamente crescente na utilidade de cada indivíduo — e obviamente respeita, sem distorção, posições de consenso perfeito. Além disso, possui outras propriedades interessantes.

Propriedade 1

A tolerância ao risco de todo o grupo, R^*, é igual à média geométrica dos parâmetros individuais de aversão ao risco, R_i:

$$\left(\prod_{i=1}^{m} R_i \right)^{1/m} = \left(\prod_{i=1}^{m} r_i^{-1} \right)^{1/m} = \left(\prod_{i=1}^{m} r_i \right)^{-1/m} = \frac{1}{r^*} = R^*.$$

Observamos que isto não aconteceria se, por exemplo, fosse considerada a média aritmética das utilidades individuais, conforme exemplo ilustrado na Figura 4.5. Neste exemplo, para $\{r_i\} = \{0.05, 0.1, 0.4, 0.8\}$, tem-se $r^* = 0.2$.

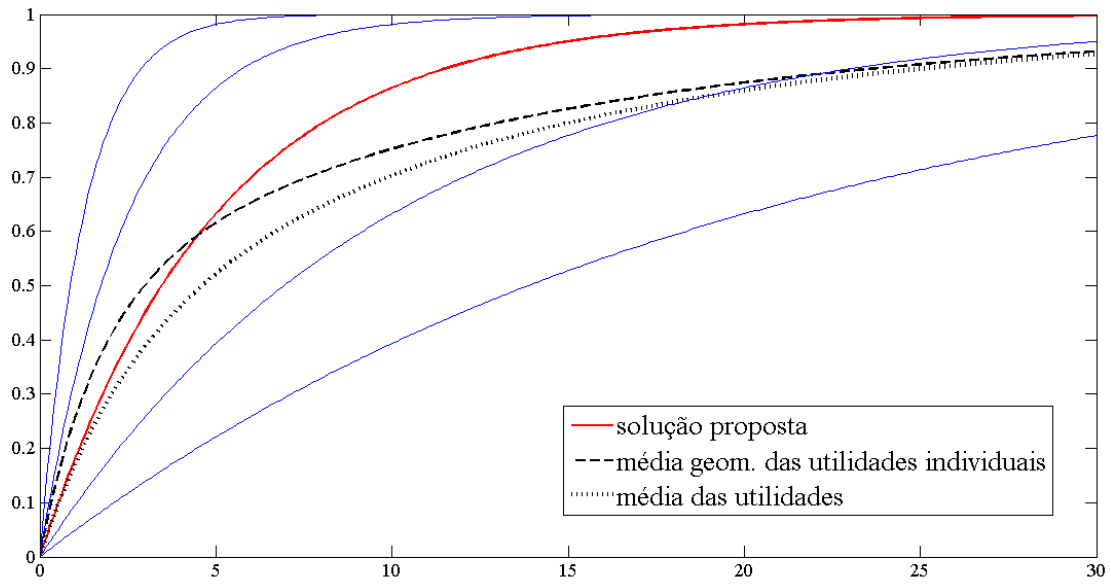


Figura 4.5 - Representação da Propriedade 1

Propriedade 2

Para cada indivíduo, considere-se a consequência q_i cuja utilidade, para esse indivíduo, é igual a um valor pré-determinado (por exemplo, $\alpha = 0.5$): $u_i(q_i) = \alpha$. Ao se tomar a média geométrica dessas consequências, $q = \left(\prod q_i\right)^{1/m}$, e pela definição acima apresentada de r^*, prova-se facilmente que a relação $u^*(q) = \alpha$ também é válida. A ilustração desta propriedade é apresentada na Figura 4.6.

Para mostrar que o resultado acima, $u^*(q) = 1 - e^{-r^* q} = \alpha$, é válido, basta mostrar que $r^* q = -\ln(1-\alpha)$. Nota-se, primeiro, que $r_i q_i = -\ln(1-\alpha)$, $\forall i \in \{1,...,m\}$. Então,

$$r^* q = \left(\prod_{i=1}^{m} r_i\right)^{1/m} \left(\prod_{i=1}^{m} q_i\right)^{1/m} = \left(\prod_{i=1}^{m} r_i q_i\right)^{1/m} = \left(\prod_{i=1}^{m} \left(-\ln(1-\alpha)\right)\right)^{1/m} = -\ln(1-\alpha)$$

Por último, e tal como é possivel constatar nas Figs. 4.5 e 4.6, a curva agregada procura não aproximar-se mais de algumas curvas individuais do que de outras. Pode conjecturar-se que ela consiste precisamente na curva que minimiza a soma dos quadrados das distâncias máximas às curvas individuais, medidas na vertical.

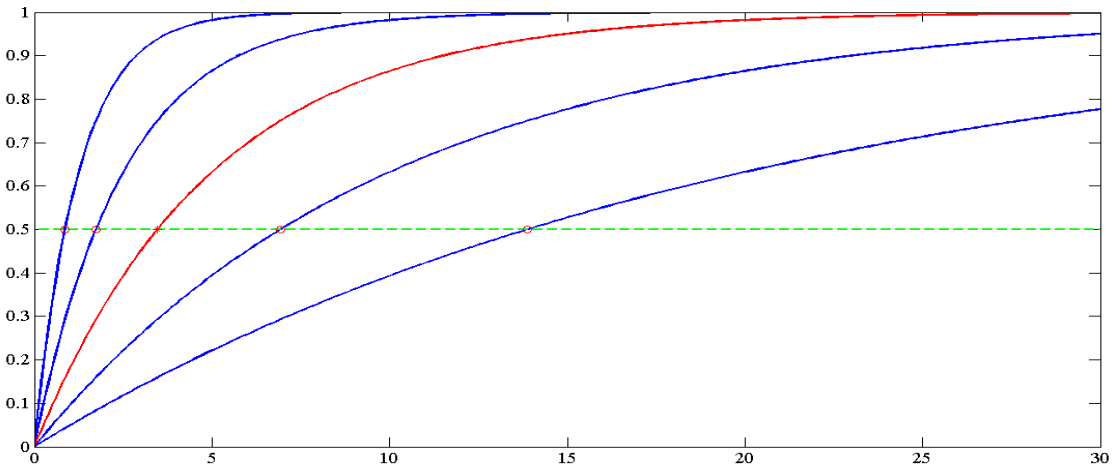


Figura 4.6 - Representação da Propriedade 2

5 AVALIAÇÃO DO RISCO DE SEGURANÇA: METODOLOGIA PROPOSTA

5.1 INTRODUÇÃO

Durante a última década, o risco de segurança perante ameaças terroristas tem sido avaliado de modo a contribuir com uma eficiente alocação de recursos finitos para combater adversários inteligentes, que adaptam os seus comportamentos em resposta às nossas próprias ações (Scouras *et al*., 2009). Basicamente, as metodologias propostas repartem-se entre o levantamento de estimativas numéricas — nomeadamente através da fórmula "ameaça x vulnerabilidade x consequências" — e a aplicação de modelos de Teoria dos Jogos.

Os pormenores e críticas a respeito dessas abordagens foram apresentados no Capítulo 2. Contudo, outras propostas têm surgido na literatura, não diretamente relacionadas com uma avaliação do risco, mas no tocante ao planeamento de medidas de proteção de áreas e sistemas críticos. Em particular, tem sido muito estudado o problema da otimização da cobertura de um espaço por redes de sensores. A maior parte das contribuições consiste, sobretudo, em técnicas de otimização da localização de sensores (Carvalho, 2013; Silva, 2013) e da configuração de redes de sensores fixos ou móveis (Wu *et al*., 2007; Caiti *et al*., 2012). Quase que invariavelmente, a literatura sobre otimização da localização de sensores só aborda o problema da maximização da cobertura de uma determinada área com um conjunto de sensores homogéneos. Nessa linha de investigação, toda a área a ser vigiada é considerada como uniformemente arriscada, sendo o risco de segurança interpretado como sinónimo da proporção da área não coberta pela rede de sensores.

Isso constitui uma lacuna grave, especialmente ao se considerar as inúmeras contribuições apresentadas no contexto de *safety risk analysis* baseadas em informações geográficas, especialmente no que diz respeito aos incêndios florestais, inundações, epidemias, etc (Verde e Zêzere, 2007; Gouldby *et al*., 2008; Raaijmakers *et al*., 2008). Analogamente, mapas (ou cartas) de *security risk* — por exemplo, mapas de risco de criminalidade — podem ser derivados a partir de registos históricos, dados demográficos, densidade espacial de ativos, recursos de vigilância, etc. Assim, consideramos um aspeto importante, por vezes negligenciado nas análises de risco de segurança perante ameaças terroristas: a provisão de *safety* pode ser usada para assegurar a *security* de um sistema. Estas duas preocupações, *safety* e *security*, concorrem para garantir a segurança de funcionamento do sistema, visto que eventuais características adversas podem suscitar perigos que podem ser explorados por uma ameaça para concretizar os seus intentos.

Problemas de risco de segurança baseados em informações geográficas podem, em geral, ser analisados a partir de uma quantidade abundante de dados. Com isso, pode ser melhor estimada uma componente chave do risco, ou seja, a possibilidade de um perigo ocorrer num determinado espaço de tempo e num determinado local. Por outro lado, são muito escassos os dados relativos a ataques terroristas em portos. Apesar disso, não é razoável que o risco de segurança seja considerado igual em todo o espaço da área a vigiar. Ainda mais, quando estamos a considerar, apenas, ameaças terroristas provenientes do meio marítimo. Neste contexto, as características ambientais predominantes afectam diretamente as potenciais intenções dos agentes terroristas, pelo que a avaliação do risco de segurança deve ser tratado como um problema de decisão sob incerteza parcial.

Considerando as questões apresentadas, propomos uma metodologia, chamada Avaliação do Risco de Segurança Espacial (*Spatial Security Risk,* SSR), baseada na elaboração de mapas de risco bidimensionais — um, correspondente a ameaças ao nível da superfície do mar, e outro, para ameaças sub-superfície. Cada mapa de risco consiste na avaliação do risco de segurança numa grelha (reticulado) espacial da forma mais objetiva possível, porém, permitindo-se que os *stakeholders* envolvidos expressem os seus juízos antes e depois do processo de otimização dos recursos de proteção. A nossa proposta não irá discutir se um porto deve ou não ter segurança reforçada, mas sim como reforçá-la, caso tenha sido tomada essa primeira decisão, de natureza político-militar. Não pretendemos estimar a probabilidade, em absoluto, de ocorrência de uma ameaça num dado período de tempo, mas sim, o de reconhecer que essa ameaça terá maior ou menor facilidade em revelar-se em diferentes partes da área de interesse a proteger. Pretendemos

avaliar como o risco está distribuído ao longo do espaço marítimo de acesso a um porto, antes e depois de uma solução para defesa desta área ser implementada, de forma a permitir uma adequada alocação de recursos.

A metodologia é inspirada numa atividade desenvolvida em âmbito militar por alguns países, como EUA e Brasil, chamada Avaliação Operacional (AO). A AO consiste num conjunto de procedimentos necessários para o fornecimento de subsídios e elementos de informação, quantitativos ou qualitativos, que possam auxiliar no processo de tomada de decisão. Esta atividade tem como propósito obter informações sobre a capacidade de um sistema cumprir as missões para as quais foi concebido em ambiente operacional tão realista quanto possível, ou seja, é um esforço para se determinar a eficácia e a adequabilidade de um sistema sob as condições mais usuais de operação.

O restante deste capítulo está organizado da seguinte forma: na secção que se segue, apresentamos uma completa descrição e comentários a respeito da metodologia proposta. Posteriormente, são apresentados os pormenores e ilustrações a respeito dos índices que definem o risco de segurança espacial. Por último, é feita uma síntese da metodologia e são apresentados exemplos ilustrativos de aplicação.

5.2 RISCO DE SEGURANÇA ESPACIAL

O acesso marítimo a um porto é uma enorme área onde navios e pequenas embarcações se movem livremente com diferentes intenções e, onde, até mesmo, atividades de lazer são realizadas. Logo, poderíamos achar que os tipos de ameaças terroristas que poderiam afetar um porto são inúmeros. No entanto, quando restringimos o problema a ameaças provenientes apenas do meio marítimo, essa definição torna-se perfeitamente plausível devido ao limitado número de ameaças que podem ser consideradas. Uma lista identificada por Radu *et al.* (2006) e Parfomak e Fritelli (2007) é apresentada na Tabela 5.1.

Tabela 5.1 - Tipos de ameaças

Ameaças
Mergulhadores
Embarcações
Veículos submarinos não tripulados
Minas derivantes

Além disso, qualquer atividade em ambiente marítimo é diretamente dependente das características dos fatores ambientais predominantes. Estas características podem servir como importantes parâmetros para analisar o grau de dificuldade que um determinado tipo de ameaça pode enfrentar para realizar um ataque bem sucedido a partir de diferentes partes de um porto. Logo, podemos concluir que diferentes zonas de um porto estão mais ou menos expostas a ameaças, devido ao grau de exposição e acessibilidade, às correntes marítimas, às características geográficas — por exemplo, quebra-mares e possíveis zonas de exclusão —, à densidade de tráfego marítimo (maior tráfego favorece ocultação), etc.

Esses fatores "ambientais" são aqui designados por Aspetos Operacionais Críticos (AOC), denominação adaptada da metodologia de Avaliação Operacional. Referem-se a fatores que originam incerteza sobre a capacidade, eficácia operacional, praticabilidade, etc de um sistema de defesa (Estado-Maior da Armada, 2004). Na Tabela 5.2 apresentamos exemplos de possíveis AOC que podem afetar o desempenho de específicas ameaças, obtidos por consulta de literatura diversa e através de entrevistas com especialistas.

Sendo assim, a implantação de recursos de defesa contra ameaças provenientes do meio marítimo pode ser apoiada pela avaliação de riscos que considera o espaço a ser protegido. A definição desse espaço, denominada Área de Interesse (*area of interest*, AoI), é peça fundamental e constitui o primeiro passo da metodologia proposta. Segundo o glossário de termos e definições militares da NATO (*NATO Standardization Agency*, 2011), AoI é uma área geográfica de preocupação para um comandante, porque está relacionada com as operações em curso ou planeadas e onde os acontecimentos poderão influenciar o cumprimento da sua missão. Na nossa proposta os limites dessa área devem ser definidos pelos agentes de decisão envolvidos.

Tabela 5.2 - Identificação de possíveis *settings*

Ameaças	Aspetos operacionais críticos			
	Intensidade das correntes marítimas	Densidade do tráfego marítimo	Temperatura da água	Largura do canal de navegação
Mergulhadores	X	X	X	X
Embarcações	—	X	—	X
Veículos submarinos não tripulados	X	X	—	—
Minas derivantes	X	X	—	X

A partir da definição da AoI, segue-se, como segundo passo da nossa metodologia, a identificação dos AOC, a identificação (escolha) dos pontos considerados críticos e a identificação das medidas de proteção já existentes. A identificação dos AOC foi objeto de discussão em parágrafos anteriores. Os pormenores sobre a escolha dos pontos considerados críticos e a verificação de medidas de proteção já existentes são discutidos no decorrer deste capítulo. Contudo, podemos resumir que pontos críticos são aqueles que, sob o ponto de vista do decisor ou decisores, são considerados como potenciais alvos de um ataque terrorista e que a verificação das medidas de proteção já existentes tem como objetivo avaliar se novas medidas são necessárias ou não.

Os dois passos apresentados anteriormente constituem a 1ª fase da nossa metodologia. A 2ª fase consiste na estimação dos índices de Suscetibilidade, Criticidade e Ineficácia, que são os elementos essenciais para avaliação do risco de segurança no espaço e são discutidos nas próximas secções. Entretanto, apresentamos uma breve descrição dos mesmos, inspirados em conceitos apresentados na Secção 2.2:

- Suscetibilidade: representa o nível de exposição natural a potenciais ataques, não levando em consideração o sistema de proteção a ser instalado;
- Criticidade: avalia o grau de perigo da presença de uma potencial ameaça num ponto da área de interesse;
- Ineficácia: avalia a potencial incapacidade do sistema de protecção lidar com uma tentativa de ataque.

Esses índices tomam valores no intervalo (0,1) e são avaliados num reticulado de pontos da área de interesse, $\mathbf{x} \in \mathrm{AoI}$. O intervalo (0,1) é usado porque os índices são definidos como utilidades, com o fim de incorporar os aspetos cognitivos e doutrinários, os objetivos e, fundamentalmente, a atitude perante o risco dos diversos *stakeholders* que compõem a administração de um porto. Como assinalado por Cox (2012), expressar o risco sob a forma de utilidades, através de uma função exponencial ou de outras formas, permite maior flexibilidade para incorporar as atitudes das pessoas diante do risco. Além disso, como pretendemos descrever o risco no espaço, a existência de uma escala intervalar é um aspeto prático para avaliar o risco antes e depois da implementação dos recursos de defesa, como resultado de um processo de otimização.

A terceira e última fase da metodologia é constituída pela representação do risco de segurança espacial através de **mapas de risco** bidimensionais — um, correspondente a ameaças ao nível da superfície do mar, e outro, para ameaças abaixo da linha da água. Um

conjunto de índices de Risco de Segurança Espacial (*SSRI*) define um mapa de risco. Os índices desse conjunto são computados num reticulado de pontos da área de interesse, $\mathbf{x} \in \text{AoI}$, através da seguinte expressão:

$$SSRI(\mathbf{x}, s) = \sqrt[3]{S(\mathbf{x}, s) \text{ x } C(\mathbf{x}, s) \text{ x } I(\mathbf{x}, s)}. \qquad \textbf{(5.1)}$$

onde *S*, *C* e *I* representam os índices de Suscetibilidade, Criticidade e Ineficácia, respetivamente, e ***s*** pode representar uma **situação** ou um ***setting*****,** conforme definições apresentadas no Capítulo 4.

A metodologia permite construir os mapas de risco sob 3 aspetos:

— O **risco-base**, ignorando quaisquer medidas de proteção atuais ou futuras, o que significa considerar $I(\mathbf{x}, s) = 1, \ \forall(\mathbf{x}, s)$;

— O **risco atual**, considerando apenas as medidas de proteção já existentes, caso existam (e os correspondentes valores de *I*);

— O **risco residual**, expectável após implementação de uma alternativa de proteção, ou seja, uma **situação** deve ser avaliada.

O objetivo será a redução dos valores da componente *I* e a consequentemente minimização, por exemplo, do valor máximo ou do valor médio de *SSRI* na AoI. A consequência de escolher uma alternativa, representada pelos dispositivos de defesa, e "acontecer" — simultaneamente ou posteriormente — um *setting* é avaliado em cada **situação**. Caso os recursos fossem ilimitados, seria teoricamente possível reduzir o risco para zero, mas as considerações de custo devem entrar também na equação. Logo, naturalmente existirá um risco residual após a implementação das medidas de proteção e a avaliação deste risco no espaço possibilita que as soluções propostas sejam melhor avaliadas — nomeadamente, através de simulação —, e eventualmente sejam revistas.

A média geométrica é utilizada para agregar as três componentes que definem o índice de Risco de Segurança Espacial pelos seguintes motivos:

— Conforme discutido no Capítulo 2, são comuns formulações para avaliação do risco de segurança baseadas no produto de 3 componentes; ocasionalmente, alguns autores fazem a agregação de tais componentes através da média aritmética. Todavia, como assinalado por Fleming e Wallace (1986), a média geométrica – e não a média aritmética – é que deve ser usada com números normalizados, independentemente da forma de como os números foram normalizados;

— Ao contrário do simples produto, a média geométrica tem a propriedade de idempotência — por exemplo, a média geométrica de {0.5, 0.5, 0.5} é 0.5;
— A média geométrica reduz a facilidade com que um baixo desempenho numa dimensão pode ser compensado noutra. Além disso, e como desejável, na hipótese de intervir um valor nulo (0), ele actua como um elemento absorvente no cálculo.

Os mapas de risco podem ajudar ao estabelecimento de perímetros de proteção de ativos considerados críticos e à escolha dos sistemas de proteção a utilizar, ou seja, servem como subsídio ao processo decisório de alocação das medidas de proteção. Esses perímetros são estabelecidos, num contexto tradicional de cunho militar-naval, por camadas concêntricas, cujos centros são, normalmente, os pontos considerados críticos. Os "raios", ou *buffers* de segurança, são definidos em função do eixo provável da ameaça, da sua velocidade e capacidade de ataque e/ou da nossa capacidade de detecção e reação atempada.

Esses perímetros podem estabelecer novas áreas dentro da AoI, incluindo, nomeadamente, as seguintes (definições adaptadas do Glossário de Termos e Definições da NATO):

— Área de Operações: definida pelo comandante da força militar, de tamanho igual ou menor que a AoI, com a finalidade de atribuir responsabilidades operacionais a determinada força ou unidade (por exemplo, um navio de patrulha), num espaço de manobra adequado e compatível com as suas possibilidades;
— Área de Vigilância: área interior à Área de Operações onde toda a atividade na superfície ou abaixo da linha da água — ou seja, embarcações, submarinos, mergulhadores, etc — deve ser detetada;
— Área de Classificação: área interior à Área de Vigilância onde a atividade na superfície ou abaixo da linha da água deve ser classificada como amiga ou hostil; pode incluir, nomeadamente, uma Área de Patrulha, para posicionamento de botes e respectivos movimentos de patrulha;
— Área crítica ou de neutralização: área próxima a pontos considerados críticos onde qualquer atividade é classificada como hostil, devendo a ameaça ser, de alguma forma, neutralizada.

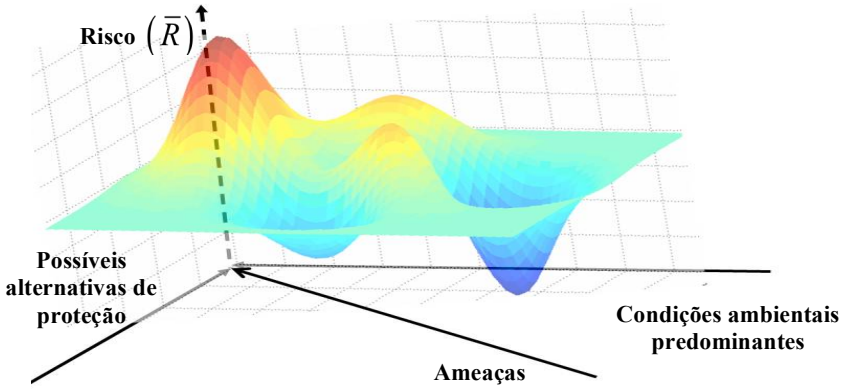


Figura 5.1 - Superfície de resposta hipotética da medida global de desempenho

Observe-se que possíveis alternativas para proteção de um porto devem ser avaliadas para todos os ***settings*** que de antemão tenham sido julgados como plausíveis. Desta forma, torna-se necessário estimar, para cada alternativa, uma medida global de desempenho representada por um escalar, $\bar{R}$, de modo a comparar as possíveis soluções. A definição de $\bar{R}$ pode, em particular, considerar uma análise de pior caso — isto é, critério Minimax de Wald — para encontrar a melhor dentro de um conjunto de possíveis alternativas de proteção. Por esta lógica, podem-se omitir todos aqueles *settings* cujos resultados são dominados por outros. Acreditamos que essa seja a melhor abordagem, devido ao elevado número de variáveis exógenas e/ou ao elevado número de níveis que podem ocorrer para algumas dessas variáveis.

A medida escalar $\bar{R}$ permitirá escolher uma configuração de recursos a utilizar, incluindo a sua composição, localização e modos de operação. A Figura 5.1 ilustra uma hipotética superfície de resposta para $\bar{R}$, em função de todas as variáveis de análise.

Nas secções que se seguem, mostramos todos os passos para definição dos índices que compõem o Risco de Segurança Espacial e apresentaremos algumas ilustrações a título meramente exemplificativo. Parte do estuário do rio Tejo será utilizado como AoI. Esta área é dividida num reticulado formado por cerca de 300 mil células, onde cada célula possui um tamanho de cerca de 30 x 30 jardas. Para cada célula são estimados os valores dos índices de Suscetibilidade, Criticidade e Ineficácia. Em geral, o tamanho de cada célula deve ser escolhido tendo em atenção a resolução dos dados geográficos disponíveis, o nível de precisão desejado, ou a própria natureza e intensidade das actividades no porto sob estudo (Ghafoori, 2013).

5.3 ÍNDICE DE SUSCETIBILIDADE

O índice de Suscetibilidade representa a propensão de uma área ser explorada por uma ameaça com o intuito de alcançar os seus objetivos, em tempo indeterminado, sendo avaliada através dos fatores de predisposição para a ocorrência das ações, não contemplando a probabilidade de ocorrência ou o seu período de retorno. Este índice é projetado para capturar o grau de facilidade de intrusão, presença e movimentação de um tipo de ameaça sob específicas condições ambientais potencialmente existentes na área de interesse de um porto.

O índice pode ser estimado a partir de múltiplos fatores, incluindo não só dados objetivos e quantificados, mas podendo também incorporar perceções subjetivas do nível de exposição natural de diferentes partes da área marítima próxima de um porto. Pode, inclusivamente, incorporar informações de inteligência militar sobre as intenções do adversário, caso existam.

A definição do índice é feita em dois níveis, conforme a Figura 5.2. O primeiro nível consiste na escolha das unidades, bem como das escalas indicando o intervalo sobre as quais os *settings* são avaliados.

Como exemplo, considere-se o *setting* formado pelo par (intensidade das correntes de maré; mergulhador). Segundo a literatura especializada e entrevistas com mergulhadores da Marinha de Portugal e do Brasil, uma intensidade de corrente maior que 2 nós pode ser considerada um limite proibitivo para uma operação de mergulho, mesmo que sejam utilizados equipamentos especiais. Com esta condição, as correntes de maré podem causar problemas consideráveis, como o aumento do consumo de ar, nadar uma distância além da planeada, perigo de emersão em local interdito, perigo de ser atingido por uma embarcação, entre outros.

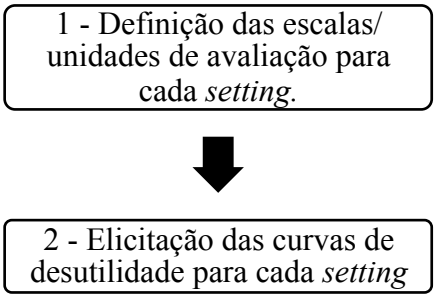
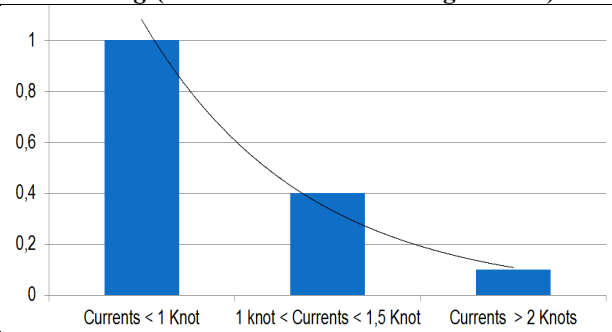


Figura 5.2 - Níveis para definição do índice de Suscetibilidade

Tabela 5.3 - Resumo do processo de definição do índice de Suscetibilidade

1ª fase			2ª fase
AOC	**Unidade**	**Escala**	**Elicitação da curva de desutilidade do *setting* (correntes de maré x mergulhador)**
Correntes de maré	**Nós (milhas/hora)**	**0 a 2 nós**	

Portanto, sob o ponto de vista dos especialistas, as zonas de um porto com correntes de maré acima de 2 nós tornam-se um obstáculo natural a um terrorista que queira alcançar os seus objetivos utilizando-se de uma estratégia de mergulho. Todavia, as correntes de maré inferiores a 2 nós não significam que o mergulho esteja isento de perigos ou dificuldades. A 2ª fase de estimação do índice de Suscetibilidade consiste na avaliação do mesmo em cada célula da AoI. As perceções subjetivas dos especialistas a respeito desse intervalo das velocidades de correntes de maré são capturadas a partir da elicitação de curvas de desutilidade utilizando-se o método proposto na Secção 4.4. As desutilidades são elicitadas sob o ponto de vista dos decisores responsáveis pela implementação dos recursos de defesa. Consequentemente, zonas de um porto com correntes próximas de 0 — isto é, maior facilidade para um mergulhador — terão desutilidades e, consequentemente, índices de Suscetibilidade iguais a 1. A Tabela 5.3 resume o processo de definição do índice de Suscetibilidade para o exemplo supracitado.

Recordemos que o nosso problema envolve um grupo de decisores e, possivelmente, de um grupo de especialistas. Pode não ser imediatamente consensual a definição das escalas ou, até mesmo, das unidades de avaliação. Nesse caso, sugerimos a utilização do método Delphi Intervalar para a construção de um consenso a respeito do intervalo de valores que limita o eixo das abcissas sobre o qual é elicitada a correspondente curva de desutilidade.

O exemplo anterior considera um *setting* com apenas um AOC: velocidade da corrente maré. Todavia, pode existir um *setting* com múltiplos AOC que em conjunto podem afectar o desempenho das ameaças — por exemplo, mergulhadores x {correntes de maré, temperatura da água}. Os agentes envolvidos nesta análise devem considerar de

antemão que algumas combinações, enquanto plausíveis, não são suficientemente preocupantes para merecer especial atenção, como, por exemplo, a análise da presença de mergulhadores numa região com águas extremamente frias.

Em resumo, o decisor deve ter um meio conveniente quer de selecionar o conjunto de AOC que compõem um determinado *setting* de interesse para a análise, quer, além disso, de atribuir-lhes pesos.

5.3.1 REPRESENTAÇÃO DO ÍNDICE DE SUSCETIBILIDADE NO ESPAÇO

A ilustração do índice de Suscetibilidade no espaço é feita para um *setting* formado por uma *pequena embarcação* como uma potencial ameaça e a *intensidade do tráfego marítimo* dentro da AoI. Note-se que uma maior intensidade de tráfego pode facilitar a presença ou até a ocultação de uma potencial embarcação terrorista, facilitando as suas intenções. As perceções subjetivas dos *stakeholders* que compõem a administração de um porto para esse *setting* podem ser avaliadas a partir de dados quantitativos disponibilizados pelo sistema de identificação automático (sistema AIS) utilizado em navios e serviços de tráfego e embarcações (VTS). A Figura 5.3 ilustra os dados em bruto do registo de trânsito de embarcações feito pelo sistema AIS para um período de três dias em parte do estuário do rio Tejo. Os pontos em azul assinalam as coordenadas geográficas onde foram registados dados de passagem de embarcações pertencentes ao sistema AIS.

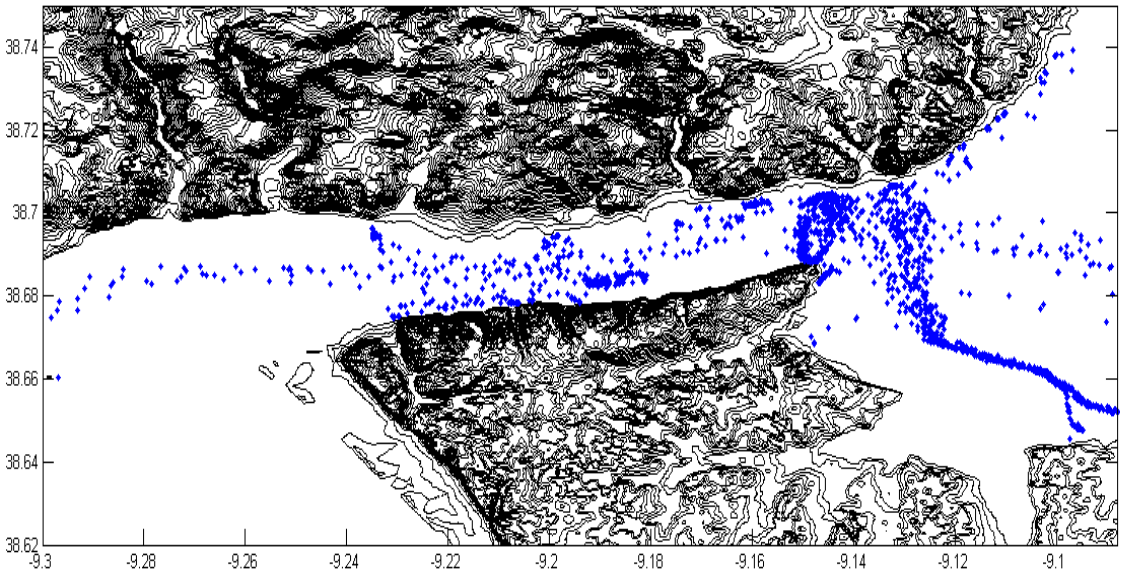
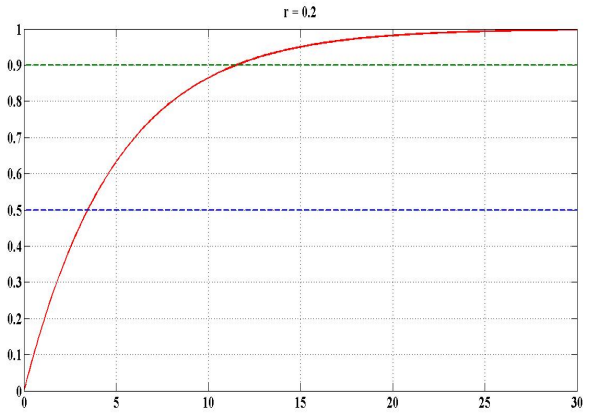


Figura 5.3 - Representação do registo do trânsito de embarcações pelo sistema AIS

Tabela 5.4 - Resumo do processo de definição do índice de Suscetibilidade para o *setting* tráfego marítimo x embarcações

1ª fase			2ª fase
AOC	**Unidade**	**Escala**	**Elicitação da curva de desutilidade do *setting***
Tráfego marítimo	**Número de navios no intervalo de 3 dias**	**0 a 30**	

De posse de dados quantitativos podemos dar início ao processo de definição do índice para cada ponto da área de interesse, ou seja: definição das escalas de avaliação do AOC tráfego marítimo e da elicitação da curva de desutilidade desse *setting* — pequena embarcação **x** intensidade do tráfego marítimo.

Consideramos como unidade de avaliação o número de registo do trânsito de embarcações recebido pelo sistema AIS em cada ponto da AoI dentro do intervalo de 60 minutos. No que concerne à escala de avaliação, foram considerados os valores de 0 e 30 como limites inferiores e superiores, respetivamente. O valor 30 foi escolhido pelo facto de ter sido o maior número registado no conjunto de dados disponível.

A Tabela 5.4 resume as fases de definição do índice de Suscetibilidade. Note-se que a curva de desutilidade foi definida a partir da interface apresenta na Secção 4.4, onde consideramos um coeficiente de aversão ao risco, *r*, igual a 0.2.

Mostramos na Figura 5.4, sob duas formas distintas, a distribuição espacial do índice de suscetibilidade no estuário do rio Tejo para o *setting* anteriormente discutido. Na Fig. 5.4(a), e de acordo com a curva elicitada da Tabela 5.4, o índice é definido como sendo zero nos pontos da AoI sem registo de dados AIS. Na Fig. 5.4(b), o índice de Suscetibilidade é fixado com o valor mínimo 0.5, atribuído nesses mesmos pontos. Este segundo procedimento é preferível, uma vez que a ausência de observações não deve ser entendida como impossibilidade de futuras observações. Desta forma, evita-se a ocorrência de valores nulos, que teriam efeito absorvente na avaliação do risco.

Existe uma grande assimetria na distribuição dos valores de tráfego observados nas diferentes células. Contudo, a aplicação da função de desutilidade indicada na Tabela 5.4, permite uma melhor gradação dos valores do índice de suscetibilidade. Além disso, foi aplicado um filtro, com base numa função *kernel,* com o fim de criar o efeito de esbatimento (*blur*) observável nas imagens da Figura 5.4.

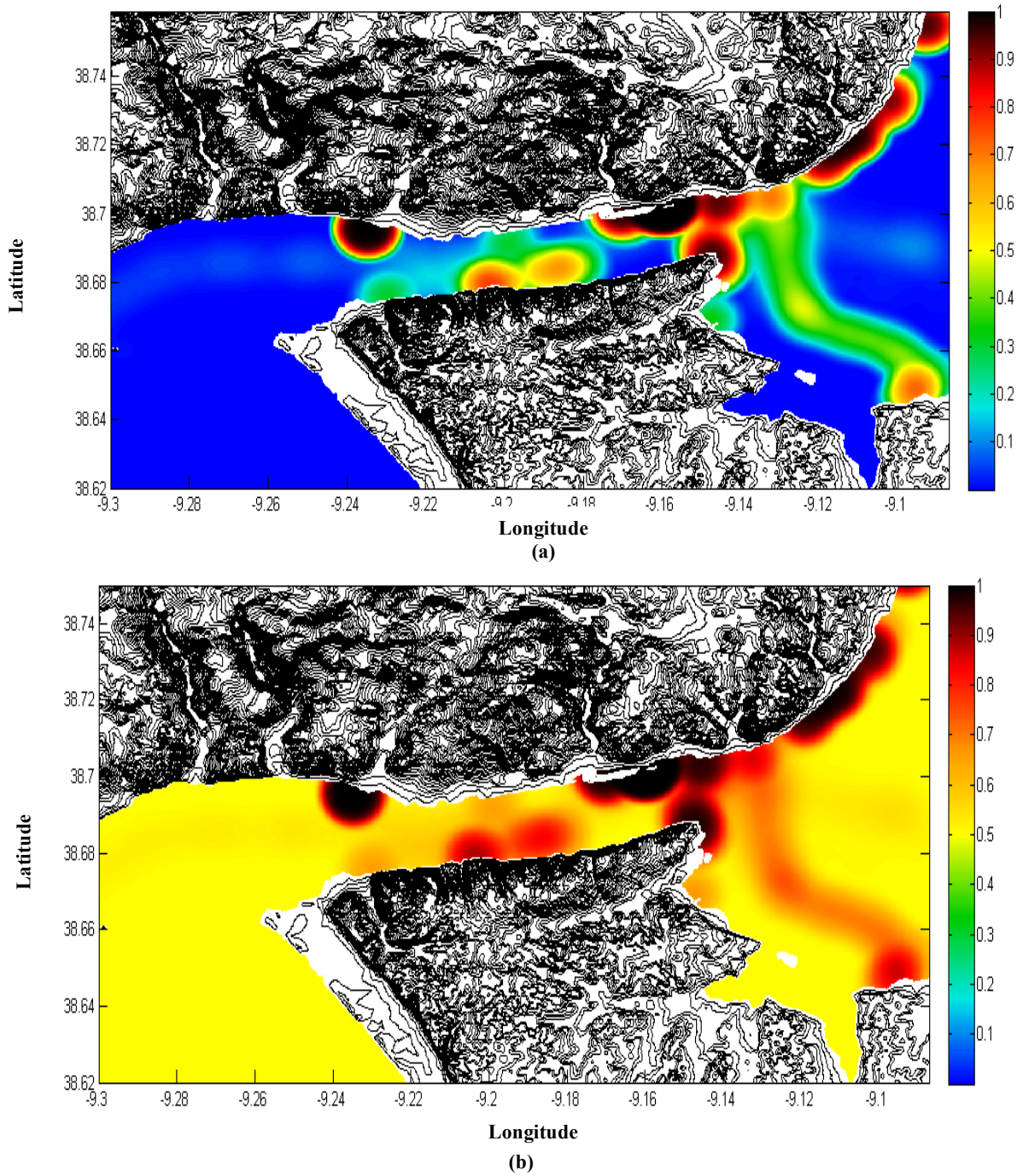


Figura 5.4 - Distribuição espacial do índice de Suscetibilidade: (a) valor mínimo do índice igual a 0; (b) valor mínimo do índice igual a 0.5

5.4 ÍNDICE DE CRITICIDADE

Esta secção discute outra componente da avaliação do risco, a criticidade. Definimos o índice de Criticidade num dado ponto da área de interesse como uma medida relativa do grau de perigosidade *percebido* da presença de uma ameaça nesse ponto. Ele será maior consoante a maior proximidade da ameaça relativamente a potenciais alvos, bem como a importância, estimada ou declarada pelos agentes de decisão, desses alvos.

O índice de Criticidade de um alvo procura condensar, num único valor, a perceção do dano resultante de um ataque bem-sucedido ao mesmo e o grau de perigo da presença de uma ameaça num ponto **x** da AoI. Desta forma, a definição do índice é dividida em duas partes:

1. A avaliação do impacto esperado de ataques bem-sucedidos a pontos declarados como críticos pelos agentes de decisão;
2. O perigo de ter uma ameaça presente em determinado local, considerando a distância a essas metas.

5.4.1 AVALIAÇÃO DO IMPACTO ESPERADO

A avaliação do impacto esperado a bens e infraestruturas, ou seja, a pontos considerados como críticos é uma preocupação manifestada pelo Código ISPS (IMO, 2003). Contudo, este regulamento não especifica como deve ser feita, constituindo, assim, uma lacuna a ser preenchida, nomeadamente, no que respeita a ataques efetuados a partir da zona molhada do porto. Aliás, a literatura é escassa no que diz respeito a essa identificação e avaliação. Uma proposta é apresentada por Parfomak e Fritelli (2007), onde é identificada uma tipologia de zonas para servir de base à identificação de pontos considerados críticos. O conjunto é formado pelos canais de navegação, áreas povoadas, terminais de passageiros, navios militares, de passageiros e de carga. Os autores também citam que a avaliação do impacto esperado de ataques bem-sucedidos a esses pontos deve ser feita a partir do ponto de vista dos líderes terroristas. Outra proposta é apresentada por Greenberg (2011) que, apesar de não mencionar quais os pontos que podem ser identificados como críticos, assinala que a avaliação das consequências deve ser estimada em função do número de potenciais mortos e feridos, danos aos ativos físicos e ao meio ambiente, além de impactos económicos e regionais.

Definimos que um "ponto" da área de interesse — por exemplo, uma infraestrutura ou um navio importante — é considerado especialmente crítico se, em caso

de um ataque terrorista bem sucedido, isso resultar numa elevada taxa de perdas ou danos bastante significativos, considerando a opinião de um ou mais *stakeholders*. A importância dos pontos críticos em termos de consequências, ou impacto expectável, de um ataque terrorista pode ser medida a partir de uma série de atributos tangíveis — tais como: perdas de vidas humanas, perdas económicas ou impacto no meio ambiente — e atributos intangíveis, como restrições a liberdades individuais e prejuízos políticos. Como mencionado por Dillon *et al.* (2009), a melhor ferramenta para agregar diferentes atributos numa única medição é a Teoria da Utilidade Multiatributo (MAUT), cujos pormenores foram apresentados no Capítulo 4.

A avaliação das consequências através da Teoria da Utilidade Multiatributo tem por objetivo fazer uma ordenação dos pontos considerados críticos, considerando diversos aspetos de perceção do risco por parte dos *stakeholders* envolvidos na gestão de um porto. Iremos agora descrever o processo de definição dos atributos que podem ser usados para mensurar as consequências de um ataque terrorista bem sucedido a um porto.

Analisando a literatura sobre avaliação de riscos de segurança em infraestruturas críticas e as normas existentes sobre proteção de portos, verificamos que o risco é um conceito multiatributo. Ou seja, as pessoas preocupam-se com um grande número de consequências, incluindo danos à vida e à saúde, à propriedade e à sociedade, e, consequentemente, todas estas preocupações devem ser incluídas na função de utilidade. Segundo Lundberg (2013), vidas perdidas e danos económicos são as consequências de maior preocupação, e são discutidas frequentemente na literatura e em análises de risco de segurança. Isto reflete não só a sua importância como, também, a relativa facilidade de usar quantidades discretas nas estimativas. Outros trabalhos identificam também outras consequências relevantes, incluindo danos ambientais, postos de trabalho perdidos, danos psicológicos, danos em símbolos para a sociedade, etc. (Mileti, 1999; Lindell e Prater, 2003; Keeney e Winterfeldt, 2010).

Note-se que esta classificação não deve ser entendida como uma simples forma de classificação dos maiores riscos. Trata-se de uma forma de prioritizar as políticas para redução de riscos, de forma a subsidiar o processo de escolha e modos de operação dos dispositivos de proteção de um porto.

Em qualquer problema de decisão, o primeiro passo é estruturar os objetivos a serem satisfeitos. Posteriormente, uma compilação de atributos deve ser feita para avaliar e mensurar esses objetivos (Keeney, 2007). Neste trabalho, referimo-nos aos objetivos como atributos, porém, cabe ressaltar que na literatura são também utilizados outros termos,

como medidas de desempenho e critérios. A especificação de atributos é uma tarefa de carácter mais técnico do que a definição dos objetivos fundamentais. Maiores detalhes a respeito deste processo são encontrados em Keeney e Gregory (2005).

Um conjunto de objetivos e atributos poderia ser construído com base no Código ISPS (IMO, 2003). Este documento menciona que as autoridades que administram um porto devem identificar e avaliar as infraestruturas e bens móveis para que se possa estabelecer a importância relativa das estruturas e instalações para o funcionamento da instalação portuária. Esta avaliação deve levar em conta a perda potencial de vidas, a importância económica do porto, o seu valor simbólico e a presença de instalações governamentais. Contudo, o Código ISPS possui lacunas, como, por exemplo, a avaliação de danos ambientais e questões mais específicas, porém importantes, num contexto em que a ameaça esperada vem do mar, como assinalado por Silva (2011). Este autor considera que uma avaliação de impacto de um ataque em diversos pontos críticos pelas autoridades portuárias poderá não corresponder a uma eventual classificação por parte de uma força naval da NATO. São organizações com objetivos diferentes: enquanto uma visa à manutenção e o desenvolvimento da actividade económica, a outra visa garantir a existência de condições para a condução de operações de forma segura.

Um dos objetivos do índice de Criticidade é avaliar o impacto de um potencial ataque terrorista a um ponto considerado crítico do porto que seja adjacente ao mar. Este objetivo fundamental pode ser dividido em subobjetivos. Os objetivos são mensurados a partir de atributos definidos em função das normas estabelecidas para proteção de portos e a tendo em atenção a literatura sobre proteção de infraestruturas críticas.

A Figura 5.5 apresenta um conjunto não exaustivo de objetivos e atributos para avaliar o impacto de um potencial ataque bem-sucedido, podendo servir de guia ou de base de reflexão para os decisores na definição de sistemas de proteção de portos.

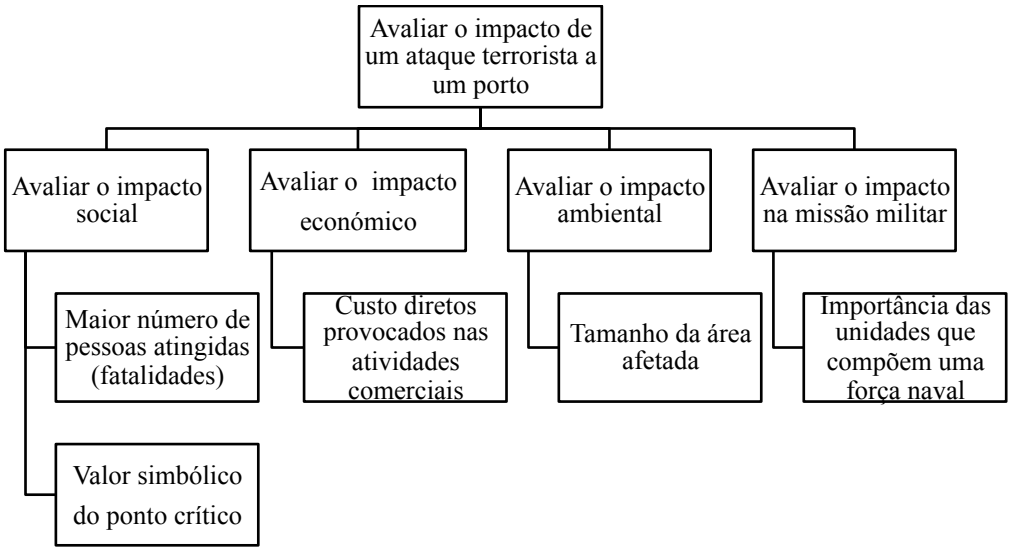


Figura 5.5 - Objetivos e atributos para avaliação do risco de segurança num porto

A análise de risco de segurança de ameaças terroristas inclui possíveis danos psicológicos, posto que um dos propósitos do terrorismo é provocar medo na população e com isso provocar mudanças na política corrente (Rosoff, 2009). Classificamos este impacto psicológico provocado na sociedade como componente do **Impacto Social**, o qual pode ser avaliado por dois atributos:

- número máximo de pessoas potencialmente atingidas no ataque, traduzido pelos números de mortos e feridos; e,
- valor simbólico dos pontos considerados críticos.

O atributo referente ao número de mortes/feridos num único episódio é considerado no trabalho de Lundberg (2013), bem como em diversos estudos de classificação de riscos. Segundo aquele autor, esse atributo é uma medida de potencial catastrófico que serve vários propósitos:

- suporta uma perspetiva diferente sobre a tomada de decisões em condições de incerteza (tais como regras de decisão minimax);
- fornece perceções sobre a assimetria da distribuição de probabilidade dos danos provocados; e,
- serve como um aspeto de atributo psicométrico de pavor.

Por outro lado, o atributo referente ao valor simbólico dos pontos críticos reflete uma recomendação do Código ISPS. Segundo este código, deve ser considerada a avaliação da importância para a sociedade de símbolos nacionais e de entidades

governamentais que possam existir na área de interesse do porto a ser protegida. Sugerimos que esta avaliação deve ser feita numa escala construída, considerando a importância de tais símbolos e entidades a nível internacional, nacional ou apenas regional.

O **Impacto económico** num contexto de *security risk* é, frequentemente, associado aos danos físicos nas instalações e à interrupção e colapso dos negócios. Interpretamos tais danos como custos diretos mensurados numa escala em unidades monetárias de um potencial dano ao ativo propriamente dito. Note-se que evitamos criar atributos em função de custos indiretos. Para estes, segundo Lundberg (2013), podem existir muitos efeitos secundários que podem variar significativamente, não somente devido às avaliações que devem ou não ser consideradas. Porém, sobretudo, devido ao facto de que os danos indiretos não são inerentes ao evento terrorista em si, refletem as escolhas individuais e políticas subsequentes ao evento. Estimar potenciais impactos indiretos depende de numerosas suposições e variáveis complexas. Além disso, como assinalado por Weil e Apostolakis (2001), a partir do ponto de vista da teoria da utilidade, a divisão só é apropriada se o decisor supuser uma independência entre os atributos.

A definição das escalas dos atributos que contribuem para avaliar o impacto económico pode estar ligada diretamente às atividades económicas desenvolvidas no porto. Segundo a atividade económica desenvolvida, um porto pode ter a seguinte classificação (Degrassi, 2001):

- Portos Comerciais: são aqueles que se limitam a receber e distribuir mercadorias, sem desenvolver atividades especializadas;
- Portos Industriais: são aqueles que desenvolvem atividades de movimentação de produtos (matéria-prima ou prefabricados) para abastecimento da indústria;
- Portos Turísticos: são aqueles voltados para atividade de turismo e entretenimento;
- Portos Pesqueiros: são aqueles utilizados para o manejo de mercadorias pesqueiras;
- Portos Multifuncionais: são aqueles que movimentam diversos tipos de cargas.

Alguns portos podem receber mais de uma classificação — Lisboa, por exemplo, é um Porto Multifuncional e Turístico. Como a avaliação de criticidade é feita para cada ponto considerado crítico, este aspeto deve ser considerado.

O **Impacto ambiental** é outra consequência reconhecida por organismos internacionais que avaliam o impacto de ataques terroristas. Para este objetivo, baseamo-nos no trabalho de Willis *et al*. (2004), que apresenta uma série de atributos para os riscos de danos ambientais, como, por exemplo: o potencial número de animais mortos, o tamanho da área do *habitat* afetado, a significância da espécie ecológica afetada, entre outros. O potencial número de animais mortos e o tamanho da área afetada podem ser avaliados segundo escalas naturais. Todavia, para o atributo relativo à significância da espécie, seria necessária a definição de uma escala construída. Os atributos podem ser descritos em diferentes formatos de contagem, tais como taxas por milhar, tempo médio entre as mortes, etc. De qualquer modo, conforme Slovic (1992) assinala, não há evidências significativas de que o formato de uma estimativa pode levar a distorções na perceção do risco em geral. Assim, sugerimos que o impacto ambiental seja avaliado pelo atributo tamanho da área afetada, devido à relativa facilidade de usar quantidades nas estimativas, além da questão já mencionada segundo a qual uma divisão só é apropriada, a partir do ponto de vista da teoria da utilidade, se o decisor supuser uma independência entre os atributos.

Por último, a avaliação de um **impacto numa missão militar** reflete uma das preocupações manifestadas no projeto SAFEPORT, citado na introdução desta tese. A missão militar refere-se a uma força naval expedicionária da NATO, atracada num porto, onde cada unidade da força tem uma missão especifica que contribui para o cumprimento da missão global. O atributo reflete, assim, aquilo que está previsto na doutrina NATO em termos de proteção de uma força:

"A proteção de uma força deve basear-se na gestão do risco. Embora não seja possível proteger todos os elementos contra todas as ameaças a todo o momento, os elementos previamente considerados **críticos para a missão** devem ser protegidos" (Silva, 2011).

Nota-se que a avaliação do impacto nos pontos críticos declarados depende do modo de ataque empregado ou, melhor, do tipo de armamento utilizado e do seu potencial de destruição. O potencial de destruição, que inclui a capacidade de letalidade, depende de uma variedade de fatores e é estudado por alguns autores, como Washburn (2000) e Lucas (2003). Uma alternativa é elicitar as opiniões de especialistas em explosivos através do Método Delphi Intervalar, tendo em conta os tipos de armamento que podem ser considerados plausíveis de serem usados por um terrorista proveniente do meio marítimo e o potencial de destruição que podem causar.

5.4.2 GRAU DE PERIGO DE UMA AMEAÇA

A segunda parte do índice de criticidade tem como objetivo definir o grau de perigo da presença de uma ameaça em diferentes partes da AoI de um porto a ser protegido. Este perigo será tanto maior, quanto maior a proximidade da ameaça aos pontos considerados críticos.

Para isso, precisamos definir uma adequada função de criticidade sobre toda a AoI, $0 < C(\mathbf{x}) < 1$. Isto pode ser gerado a partir de um conjunto limitado de informações, incluindo:

— um conjunto de máximos locais, chamados pontos críticos, $\{\mathbf{g}_i\}_{i=1,...,m}$;

— os correspondentes valores da avaliação multiatributo, $0.5 < \gamma_i < 1,\ i = 1,...,m$, discutidos na subsecção anterior.

Segundo Rodrigues (2012), pode ser associada uma função, $0 < C_i(\mathbf{x},\lambda) \le \gamma_i$, a cada ponto crítico, $\mathbf{g}_i$, com valores decaindo com a distância ao ponto crítico de um ponto qualquer **x** dentro da AoI (possível posição de uma ameaça). Concretamente, essa função pode ser definida por:

$$C_i(\mathbf{x},\lambda) = \frac{\lambda\gamma_i}{\lambda + \left\|\mathbf{x}-\mathbf{g}_i\right\|},\ 0.5 < \gamma_i \le 1 \qquad \textbf{(5.2)}$$

onde λ é o parâmetro que regula a taxa de decaimento da superfície (em função da distância), γ_i é o valor da avaliação multiatributo do ponto considerado crítico, $\mathbf{g}_i$, e $\left\|\mathbf{x}-\mathbf{g}_i\right\|$ é a distância, por via marítima, entre **x** e $\mathbf{g}_i$. Assinalamos que a presença de quebra-mares ou outros obstáculos acarreta que uma linha reta nem sempre é o caminho mais curto entre um ponto **x** e um ponto considerado crítico, $\mathbf{g}_i$.

A função de criticidade global, isto é, a função que vai permitir representar a distribuição do índice de Criticidade por todo o espaço da AoI, é o resultado da combinação dessas funções individuais segundo a fórmula:

$$C(\mathbf{x}) = 1 - \prod_{i=1}^{m}\left(1 - C_i\left(\mathbf{x},\lambda^*\right)\right) \qquad \textbf{(5.3)}$$

para um valor apropriado λ^*, a determinar.

Note-se que o valor definido para um ponto **x** relativamente próximo de, pelo menos, um ponto crítico, é mais elevado — isto é, o perigo da presença de uma ameaça naquela posição é maior. Além disso, embora $C_i\left(\mathbf{g}_i,\lambda\right) = \gamma_i,\ \forall\lambda > 0$, tem-se, para $m = 2$,

$C(\mathbf{g}_i) > \gamma_i$. Em particular, a presença de uma ameaça numa posição relativamente próxima de pelo menos dois pontos considerados críticos vai representar um perigo significativo para ambos os pontos.

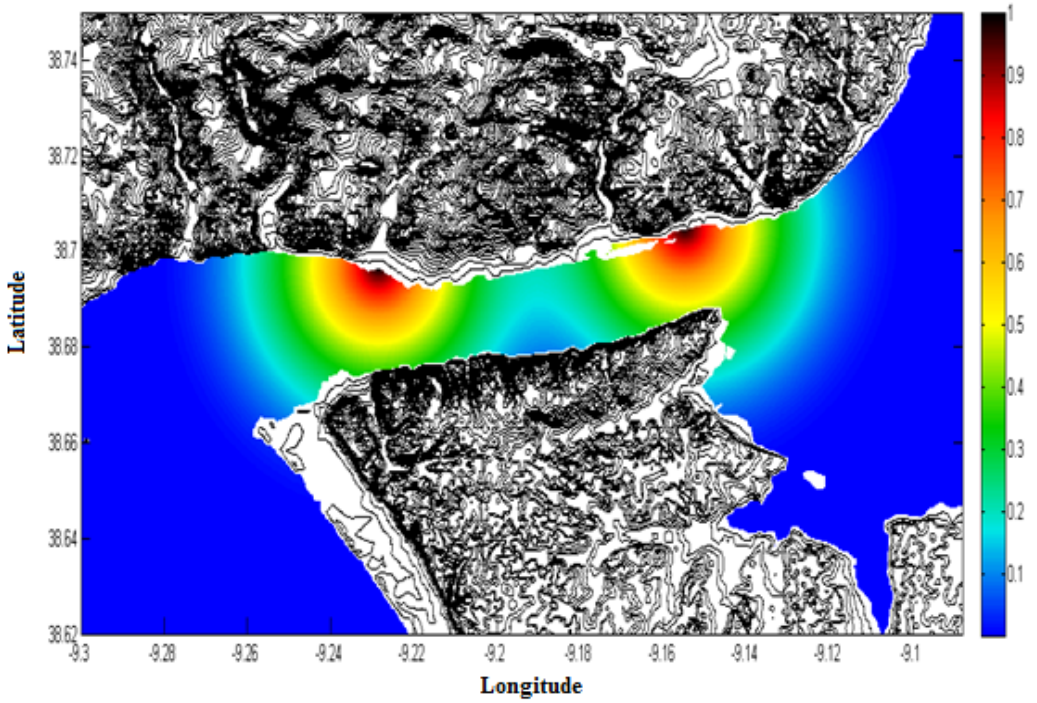
Os valores de criticidade sobre toda a área de interesse estão compreendidos entre um valor máximo, $C_{\max}$, com $\max\{\gamma_i\} \le C_{\max} < 1$, e um mínimo, $\gamma_0 = C_{\min} > 0$. Este valor mínimo, geralmente atingido num ponto consideravelmente distante dos pontos críticos, é um nível base da criticidade sobre toda a AoI, menor que $\min\{\gamma_i\}_{i=1,\ldots,m}$. Em certo sentido, traduz o nível base de alerta na AoI. O seu valor deve ser estabelecido pelos agentes de decisão, por exemplo, recorrendo ao Método Delphi Intervalar. Note-se que, uma vez definido o valor de γ_0, a restrição $C_{\min} = \gamma_0$ induz, de forma unívoca, um valor de λ^*, ficando a definição da função da Eq. 5.3 completamente determinada.

5.4.3 REPRESENTAÇÃO DO ÍNDICE DE CRITICIDADE NO ESPAÇO

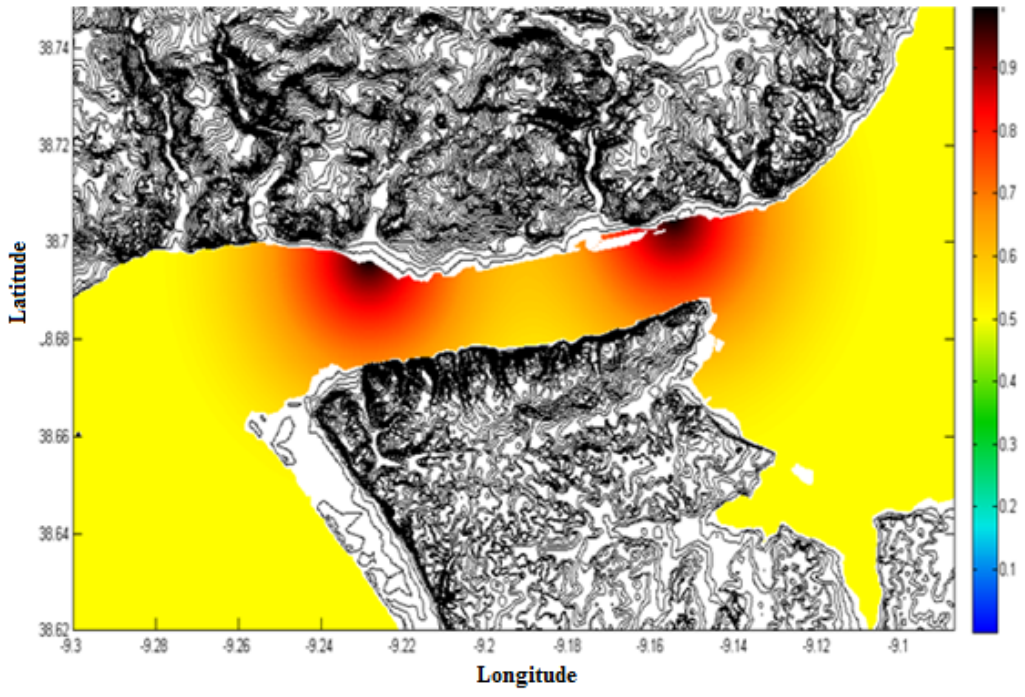
Nesta subsecção, apresentamos alguns exemplos ilustrativos da representação do índice de Criticidade no espaço. Consideramos dois pontos críticos em duas diferentes localizações da área de interesse formada por parte do estuário do rio Tejo. No primeiro exemplo, os dois pontos críticos estão localizados na margem norte e, no segundo, um ponto está na margem norte e outro na margem sul. Por simplicidade, os valores multiatributo dos pontos críticos foram fixados iguais: $\gamma_i = 0.9$.

Em relação ao grau de perigo da presença de uma ameaça num ponto da área de interesse, foram escolhidos dois valores base. As Figuras 5.6 (a - d) ilustram a distribuição do índice de criticidade no espaço da área de interesse para os dois pontos críticos já mencionados, sendo que, em (a) e (c), $\gamma_0 = 0.01$, enquanto em (b) e (d), $\gamma_0 = 0.5$.

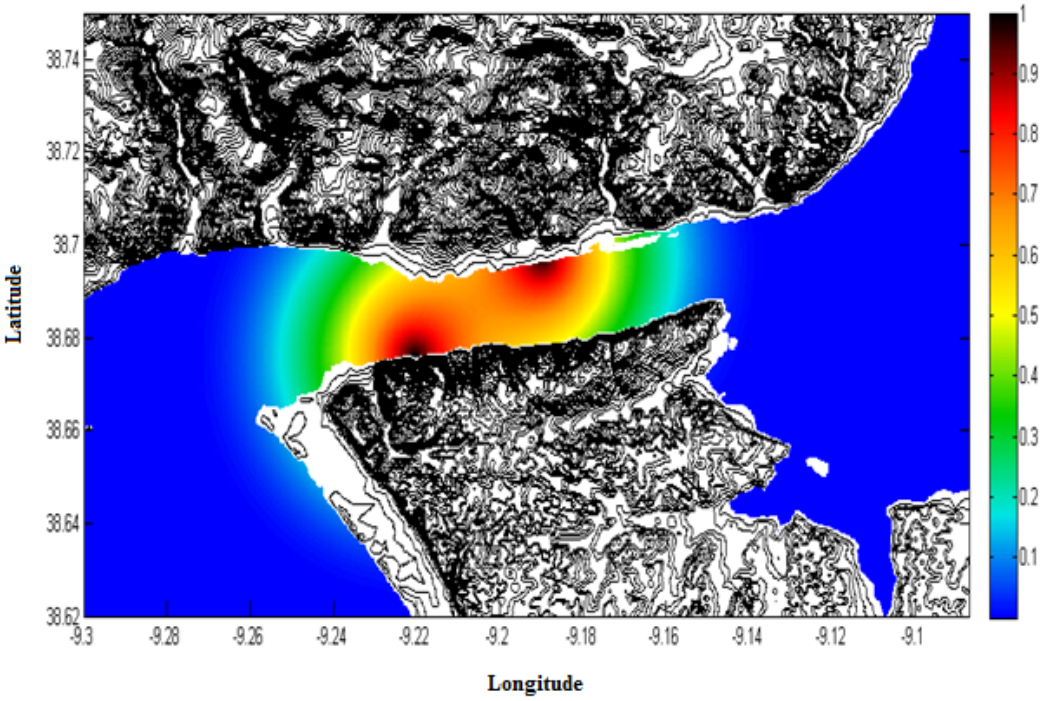
Podemos observar nas figuras que as cores com tonalidades vermelhas representam os mais altos valores para o índice, ou seja, representam um espaço da área de interesse onde a presença de uma ameaça seria interpretada como o mais alto grau de perigo. Outra característica dessas figuras está relacionada com o facto de que o grau de perigo de uma ameaça localizada a uma mesma distância de ambos os pontos é o mesmo. Este efeito confirma os comentários apresentados no final da subsecção anterior.


Latitude
38.74
38.72
38.7
38.68
38.66
38.64
38.62
-9.3
-9.28
-9.26
-9.24
-9.22
-9.2
-9.18
-9.16
-9.14
-9.12
-9.1
Longitude
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1

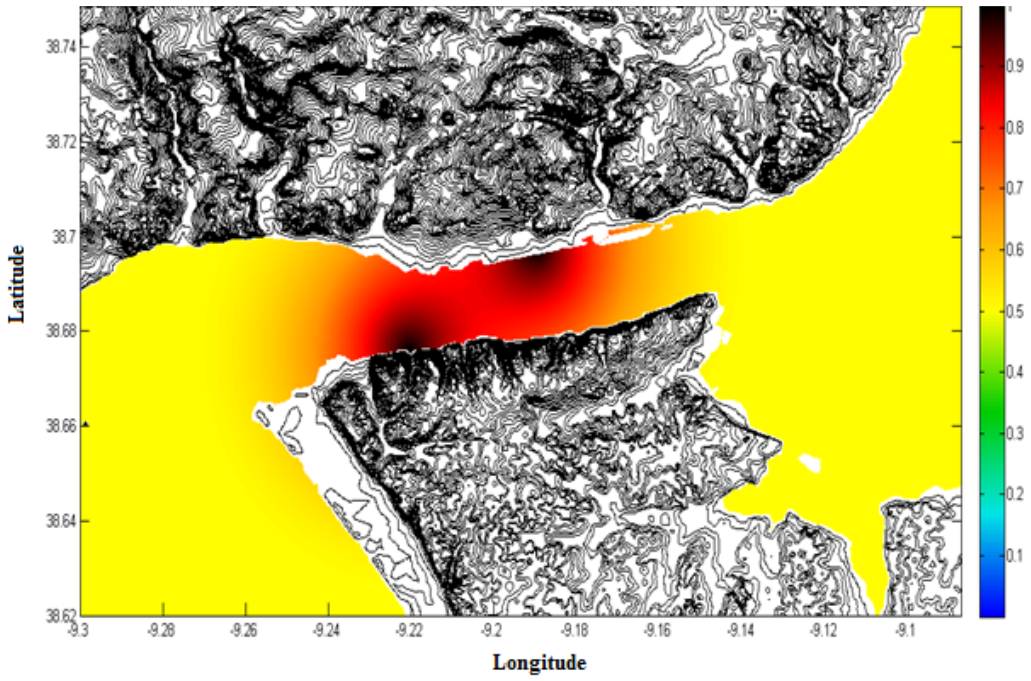
(a)


Latitude
38.74
38.72
38.7
38.68
38.66
38.64
38.62
-9.3
-9.28
-9.26
-9.24
-9.22
-9.2
-9.18
-9.16
-9.14
-9.12
-9.1
Longitude
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1

(b)



(c)



(d)

Figura 5.6 - Distribuição espacial do índice de Criticidade para dois pontos críticos: (a) e (c) valor base igual a 0.01; (b) e (d) valor base igual a 0.5

5.5 ÍNDICE DE INEFICÁCIA

A ineficácia pode ser definida como a incapacidade do sistema de defesa conseguir lidar com uma tentativa de ataque. Tomamos, como exemplo, um mergulhador com uma velocidade média de 1 nó. A esta velocidade, uma distância de 500 metros pode ser percorrida em cerca de 17 minutos. Esses 500 metros são na realidade a distância de deteção para sistemas de sonar concebidos para a deteção de mergulhadores com uma probabilidade de deteção teórica de mais do que 90%, considerando uma relação sinal/ruído de -25 dB. Se considerarmos ainda o tempo necessário para a deteção, identificação, classificação e possível neutralização da ameaça, o tempo necessário para todo o processo pode ficar em torno de 8 a 10 minutos, intervalo de tempo que pode ser considerado crítico (Radu *et al*., 2006).

Pela leitura do parágrafo anterior, podemos depreender que um sistema de proteção de um porto, no contexto de ameaças terroristas, deve ser constituído por sensores fixos e móveis, como por exemplo, radares, sonares, sensores eletro-ópticos e botes-patrulha. Em suma, o sistema deve ser capaz de detetar o contacto o mais distante possível do alvo, de modo a perceber o ambiente e reconhecer se uma possível ameaça está ocorrendo dentro de um perímetro de proteção.

Sendo assim, a ineficácia de um sistema de defesa poderia ser avaliada a partir de parâmetros utilizados na metodologia usada pelo Departamento de Defesa dos Estados Unidos (Dillon *et al.*, 2009). A metodologia mede a capacidade de proteção de um ativo considerado crítico relativamente a várias capacidades, em sucessão: detetar, avaliar, avisar, defender. Estes parâmetros são, na maioria dos casos, probabilidades definidas por especialistas no assunto, sendo, desta forma, a capacidade do sistema medida pelo modelo probabilístico:

$$1 - \mathrm{P}(\textit{Detetar} \mid \textit{Ataque}) \times \mathrm{P}(\textit{Avaliar} \mid \textit{Detetado}) \times \mathrm{P}(\textit{Avisar} \mid \textit{Avaliado}) \times \mathrm{P}(\textit{Defender} \mid \textit{Avisado})$$

Respetivamente, em sucessão: detetar a ameaça dado que o ataque foi iniciado; identificar correctamente um contacto como hostil ou amigo, dado que ele foi detetado; avisar os dispositivos de defesa de um ataque iminente dado que o contacto foi identificado correctamente como hostil; e, interditar o caminho de uma ameaça em direcção ao alvo dado que os dispositivos de defesa foram avisados.

Contudo, pretendemos desenvolver uma metodologia para a avaliação de riscos que permita uma avaliação subjetiva dos agentes de decisão ou especialistas no assunto a

partir da avaliação de dados quantitativos conhecidos. Assim, podemos afirmar que, entre todos os parâmetros citados anteriormente, a probabilidade de deteção de uma potencial ameaça é um valor perfeitamente mensurável. Além disso, a detecção é o ponto de partida para as medidas subsequentes; sem a detecção de uma potencial ameaça, as outras medidas são inexequíveis.

Considere-se um sistema de vigilância com *n* sensores fixos localizados nas posições $\mathbf{c}_1, \mathbf{c}_2, ..., \mathbf{c}_n$. Cada sensor *i* possui uma função de probabilidade de deteção, $D_i(\mathbf{x})$, avaliada em todos os pontos **x** da AoI. Alguns modelos fazem uma simplificação desta abordagem considerando apenas regiões circulares com raio *r* onde a deteção é garantida:

$$\begin{cases} D_i(\mathbf{x}) = 1, \text{ se } \left\|\mathbf{x} - \mathbf{c}_n\right\| \le r \\ 0, \text{ caso contrário} \end{cases}$$

Porém, é mais razoável considerar modelos probabilísticos de deteção, $0 \le D_i(\mathbf{x}) \le 1$, que fornecem estimativas de probabilidades que degradam com a distância.

A avaliação da probabilidade de deteção de um objeto presente numa posição $\mathbf{x}$ por um sensor localizado em $\mathbf{c}$ pode ser modelada por uma função devidamente parametrizada. Por exemplo, Chung *et al*. (2011), entre outros autores, consideraram o chamado modelo *Poisson Scan* para descrever a função de probabilidade de detecção de um mergulhador por um sonar:

$$D_{\mathbf{c}}(\mathbf{x}) = \lambda \Phi\left(\frac{F - \rho(\mathbf{c},\mathbf{x})}{\sigma}\right)$$

onde:

λ : taxa de oportunidade de detecção, de acordo com um processo de Poisson;

Φ : função de distribuição da Normal *standard*;

ρ : perda de sinal, em função da distância, por exemplo: $\rho(\mathbf{c},\mathbf{x}) = a\left\|\mathbf{c} - \mathbf{x}\right\|^2 + b$

F, σ, a, b: parâmetros específicos do sensor (modelo de sonar).

Na Figura 5.7 é mostrado um exemplo da superfície de probabilidade de deteção decorrente daquele modelo, com $\lambda = 1; F = 70; \sigma = 5; a = 0.5; b = 60$. Como se constata, a função é radialmente simétrica e estritamente decrescente com o aumento da distância.

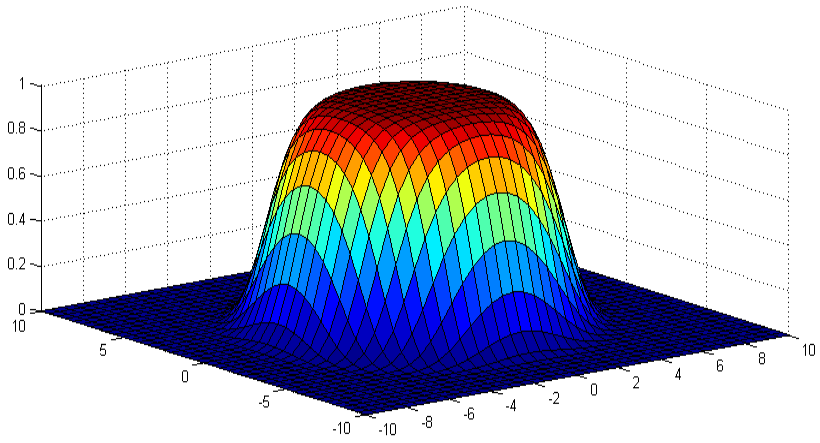


Figura 5.7 - Forma típica de uma função *Poisson-Scan*

Para outros tipos de sensores, a superfície de avaliação da capacidade de deteção pode ter formatos semelhantes, algo diferentes ou, até, substancialmente diferentes. Uma ampla revisão de técnicas para mensurar a probabilidade de detecção de sensores vai além do âmbito deste trabalho. O nosso objetivo aqui é apenas destacar os principais conceitos e questões, pelo que se sugere a consulta de Wagner *et al*., (1999) e Washburn (2002). Contudo, segundo Caiti *et al*. (2012), mesmo modelos genéricos, válidos apenas para condições ambientais "normais", podem ser úteis para analisar de forma rápida o desempenho de uma configuração preliminar do sistema de vigilância.

Independentemente do modelo, a probabilidade conjunta de deteção de um alvo numa posição **x** por, no mínimo, um de entre *n* sensores instalados, assumindo que são independentes, é dada por:

$$D(\mathbf{x}) = 1 - \prod_{i=1}^{n} \left(1 - D_i(\mathbf{x})\right). \qquad \textbf{(5.4)}$$

Como já explicado, o tempo decorrido desde a deteção até ao engajamento do alvo deve ser suficiente para permitir a reação do sistema de combate como um todo, pois, caso contrário, a ameaça poderá atingir o alvo antes que os sistemas de defesa possam neutralizá-la. Além disso, as diferentes condições ambientais podem influenciar diretamente o desempenho dos diversos tipos de sensores, fixos ou móveis, que podem ser utilizados num sistema de vigilância de um porto. Por exemplo, a capacidade de um sensor eletro-óptico é afetada pela posição do sol, pela existência de chuva, pelo estado da superfície do mar, etc. Também a capacidade de um radar ou de um sonar são diretamente

afetadas pelas condições ambientais e pelas características físicas do alvo, no que diz respeito à sua detetabilidade.

Logo, a avaliação do desempenho do sistema pela função da Eq. 5.4 pode não ser suficiente para os agentes de decisão. Isto é, a função de avaliação da probabilidade de deteção de um sensor ou de um conjunto de sensores fornece valores isolados cujas consequências podem ser interpretadas pelos agentes de decisão de diversas formas. Sendo assim, a definição de utilidades para as probabilidades de deteção em função da distância é a forma abordada neste trabalho para contornar este problema. Esta abordagem visa incorporar no problema as escolhas dos agentes de decisão e o seu comportamento em relação ao risco em função das circunstâncias específicas de quem faz a estimativa.

A partir dos argumentos citados, definimos o índice de Ineficácia da seguinte forma:

$$I(\mathbf{x}) = 1 - u\left(D(\mathbf{x})\right). \qquad \textbf{(5.5)}$$

onde $u\left(D(\mathbf{x})\right)$ é a *utilidade* da probabilidade de deteção para um ponto $\mathbf{x} \in \mathrm{AoI}$.

A elicitação de uma função de utilidade do grupo para as probabilidades de deteção pode seguir a proposta apresentada na Secção 4.4, caso o grupo tenha uma atitude de aversão ao risco. Porém, devido às pequenas alterações nos valores das probabilidades de deteção, o decisor pode demonstar atitudes perante o risco representadas por outros tipos de funções de utilidade, por exemplo, uma função de utilidade linear por partes, ou, até mesmo, pode assumir uma atitude de indiferença ao risco.

Uma alternativa para a avaliação dessas probabilidades é a baseada no método descrito por Jiménez *et al*. (2003). Nesta proposta, os autores apresentam um sistema de apoio à decisão que permite ao decisor usar uma escala subjetiva sem definir uma função de utilidade propriamente dita *a priori*, implementada no sistema através de uma escala "termómetro" cujos valores mínimos e máximos são 0 e 1, indicando respetivamente o pior e o melhor casos. O sistema desenvolvido não aborda a problemática da elicitação das preferências de um grupo. Nesta situação, o Método Delphi Intervalar poderia ser utilizado, ou seja, também poderíamos empregar uma escala subjetiva, porém, permitindo-se que cada decisor estabeleça as suas preferências através de um intervalo para cada probabilidade de deteção.

5.5.1 REPRESENTAÇÃO DO ÍNDICE DE INEFICÁCIA NO ESPAÇO

Mostramos nesta subsecção dois exemplos que representam a distribuição do índice de ineficácia no espaço da AoI, visualizados nas Figuras 5.8(a,b).

Em cada exemplo, consideramos um sistema de proteção formado por dois radares hipotéticos que estão localizados na margem sul e na margem norte do estuário do rio Tejo, em diferentes posições. A representação é compatível com o que permitiu estimar o mapa de suscetibilidade: tráfego à superfície (Fig. 5.3) e não "tráfego abaixo da linha da água".

As funções de probabilidade de detecção dos radares foram adaptadas de Mahafza (2002). Essas funções geradas apresentaram um aspeto radialmente simétrico e estritamente decrescente com a distância, próximas da ilustrada na Fig. 5.7. Além disso, para a definição do índice de Ineficácia, de acordo com a função da Eq. 5.5, foi considerada uma função de utilidade "neutra" — isto é, a simples função identidade, sem alteração dos valores das probabilidades fornecidas pelo modelo do sensor.

Optamos por ilustrar dois exemplos da distribuição do índice de Ineficácia no espaço para permitir a visualização do efeito que pode ser causado em função da proximidade das localizações de eventuais sensores, no caso ilustrado dois radares. Assim, devido à proximidade das suas localizações, podemos observar na Figura 5.8(b) pontos de intersecção do índice de ineficácia dos dois radares, facto que não ocorre na Figura 5.8(a).

Cabe ressaltar que partimos do princípio que os radares hipotéticos estão localizados em posições que permitem superar eventuais obstáculos à linha de vista, como por exemplo, o contorno da linha de costa ou pontes. Tais obstáculos podem provocar um "corte" nas superfícies de detecção e devem ser considerados na avaliação do índice de Ineficácia no espaço da AoI.

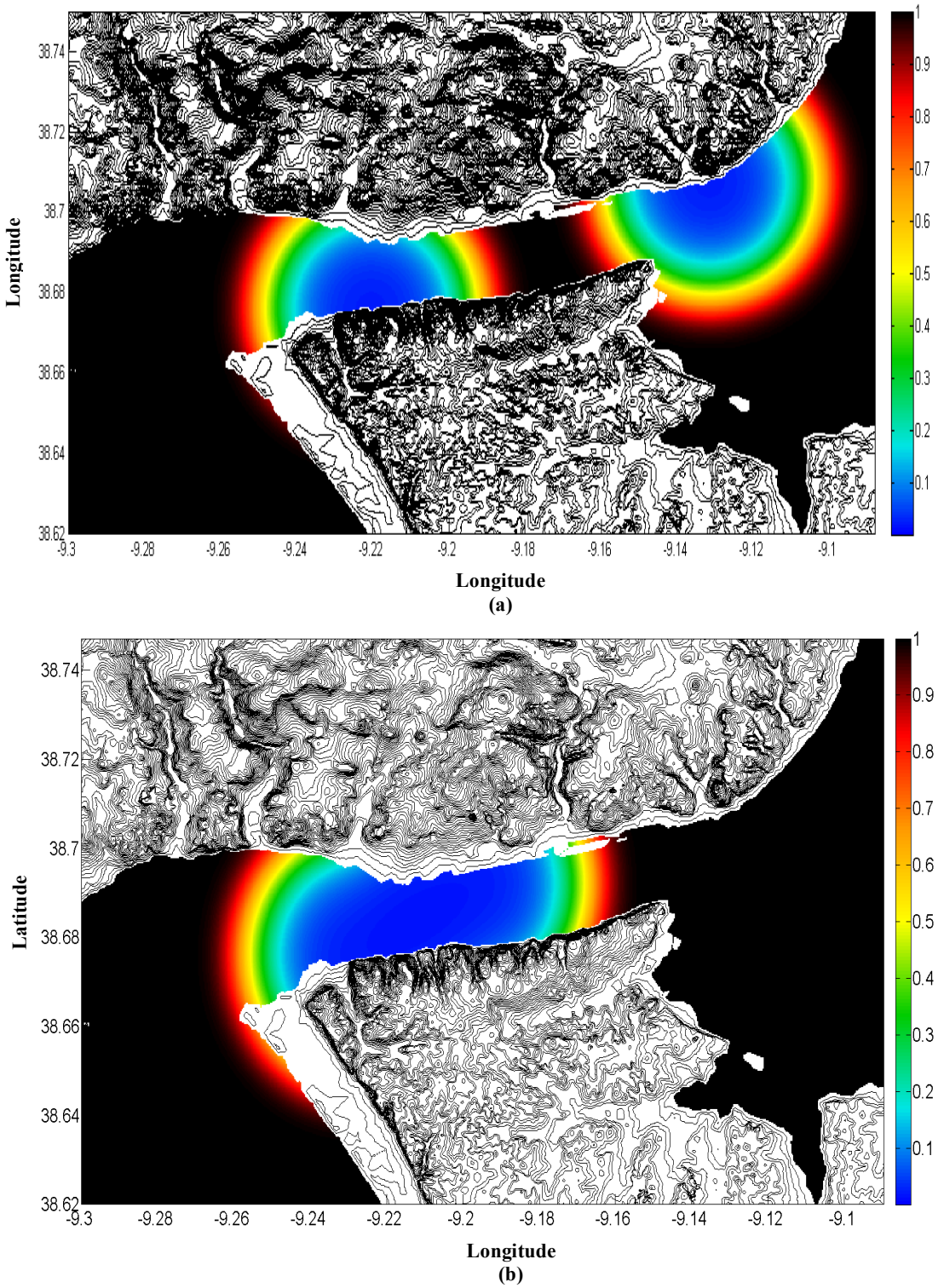


Figura 5.8 - Representação do índice de Ineficácia no espaço para um sistema de proteção formado por dois radares em diferentes localizações

5.6 SÍNTESE E ILUSTRAÇÃO DO RISCO DE SEGURANÇA ESPACIAL

Apresentamos neste capítulo a metodologia geral de avaliação do Risco de Segurança Espacial, cujo objetivo é apoiar o processo decisório para alocação de recursos de protecção de um porto contra ameaças terroristas provenientes do meio marítimo. A metodologia permite a visualização da distribuição do risco na AoI através de **mapas de risco bidimensionais** — um correspondente a ameaças ao nível da superfície do mar, e outro, para ameaças abaixo da linha da água.

Um mapa de risco é definido por um conjunto de índices de risco de segurança espacial (*SSRI*), calculados a partir da média geométrica de 3 índices componentes num reticulado de pontos da AoI. Concluímos que esses mapas de risco servem como subsídio para um processo de otimização da localização dos recursos de protecção, considerando quer restrições de custo quer o grau de cobertura dos sensores. Também podem ser utilizados como base para um decisor introduzir requisitos mais específicos no sistema de proteção em função dos perímetros de proteção que sejam estabelecidos. Por exemplo, citamos a especificação dos sensores, modo de funcionamento ou, até mesmo, as restrições impostas à admissibilidade das localizações. A metodologia está organizada sob uma estrutura hierárquica que pode ser visualizada na Figura 5.9.

Em seguida, apresentamos na Figura 5.10 dois mapas de risco-base de segurança espacial, correspondentes a ameaças ao nível da superfície do mar. Na construção desses mapas utilizamos os dados concernentes ao conjunto de índices de Suscetibilidade representado pela Fig. 5.4(b) e, especificamente, no tocante ao índice de Criticidade, utilizamos os conjuntos definidos para um valor de $\gamma_0 = 0.5$ com dois pontos críticos, conforme a Figura 5.6(d).

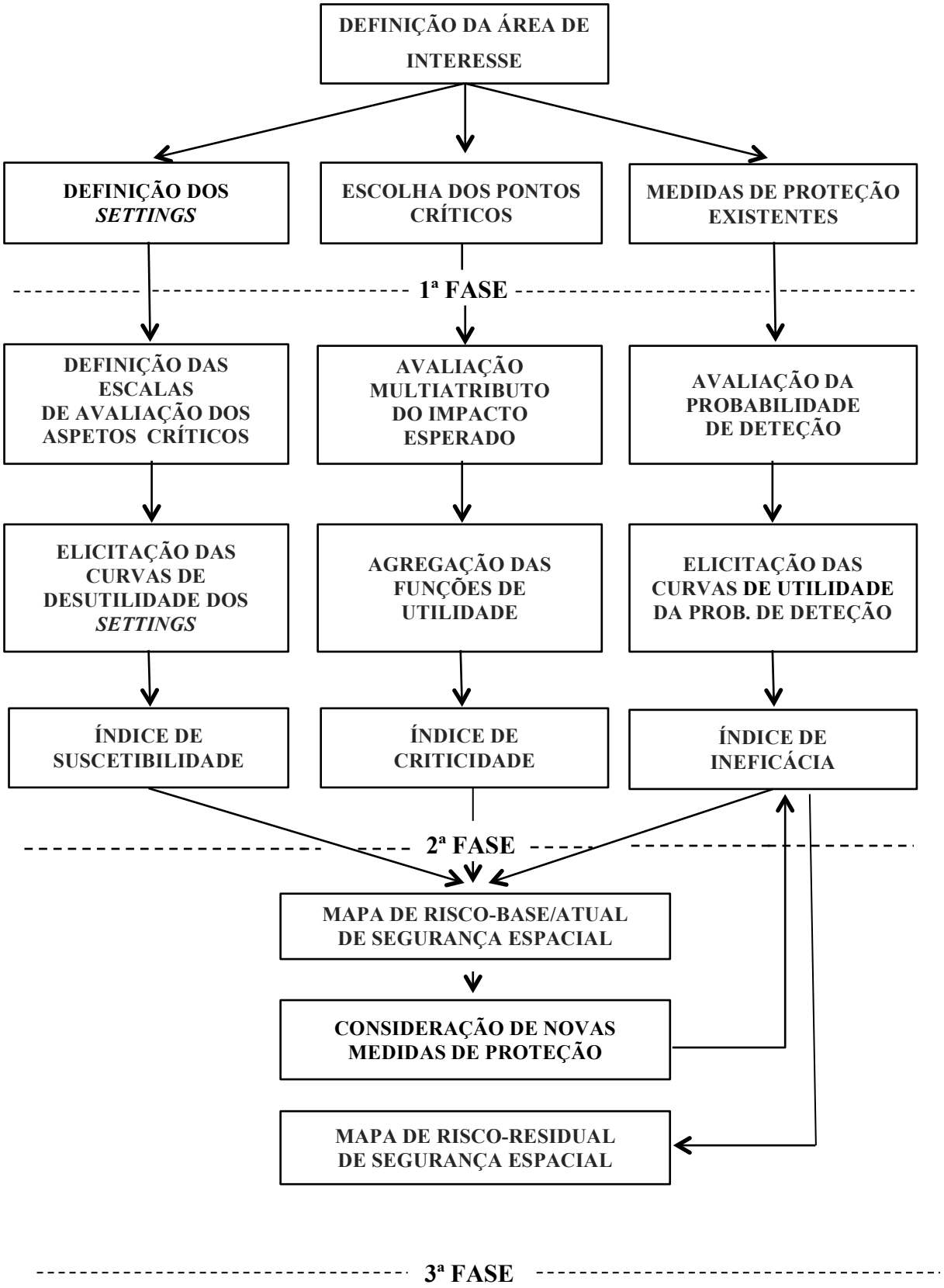
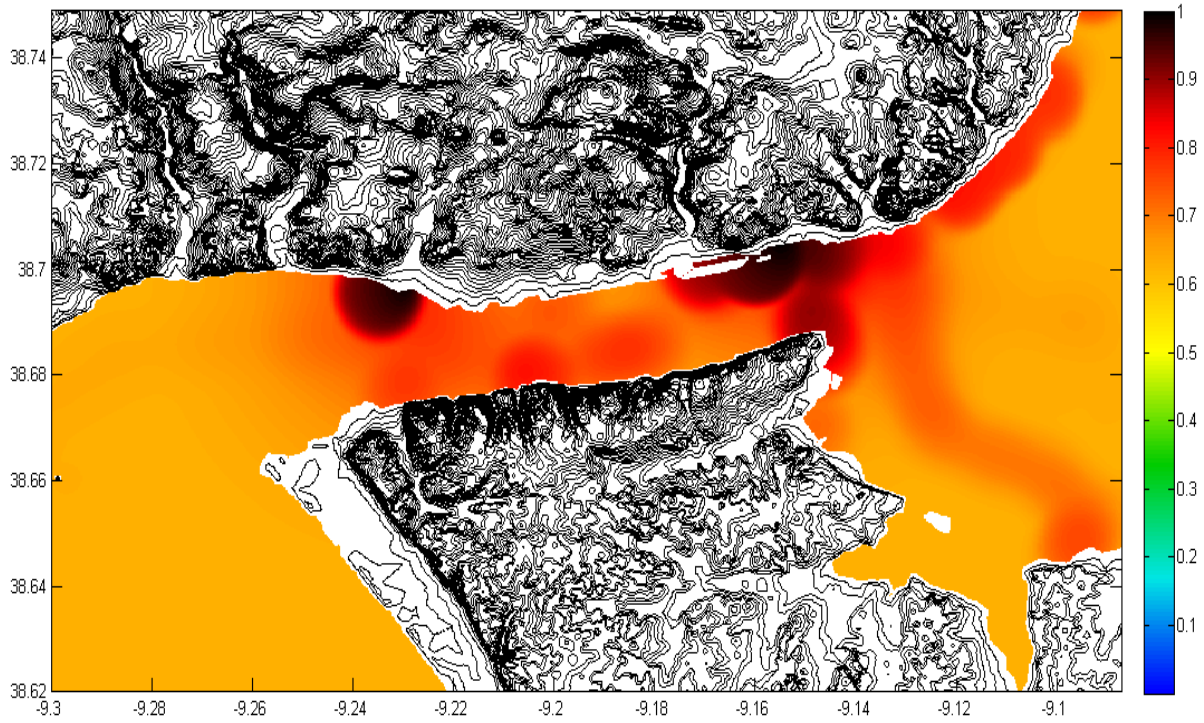
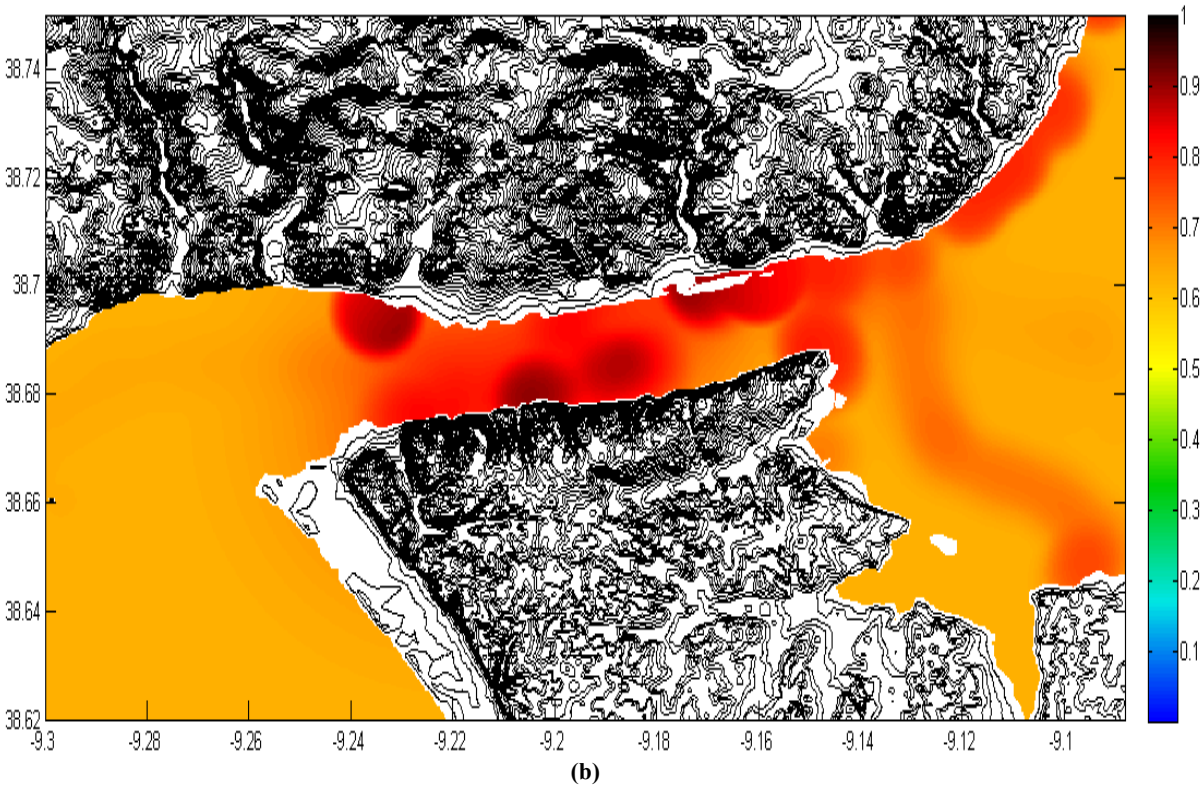


Figura 5.9 - Estrutura hierárquica da elaboração de um mapa de Risco de Segurança Espacial



(a)



(b)

Figura 5.10 - Representação do risco-base de segurança espacial: (a) dois pontos críticos na margem norte; (b) um ponto crítico na margem Norte e outro na margem Sul

A partir da análise das Figs. 5.10(a,b), podemos concluir:

— Os valores do índice SSRI distribuem-se entre aproximadamente 0.6 e 1;

— Em (a), o mapa de risco apresenta uma maior densidade de pontos com índices de risco próximos de 1;

— Tanto em (a) quanto em (b), as zonas com índices de risco mais elevados poderiam servir de base para a definição de áreas de patrulha; são zonas próximas dos pontos críticos ou onde o índice de suscetibilidade é elevado;

— Os pontos da AoI com os menores índices de risco são aqueles mais distantes dos pontos críticos e onde o índice de suscetibilidade é igual a 0.5.

De modo a permitir uma comparação e melhor compreensão das conclusões citadas anteriormente, apresentamos na Figura 5.11 os mapas dos índices de Suscetibilidade e de Criticidade cujos dados utilizamos para a construção do mapa de risco-base apresentado na Figura 5.10(b).

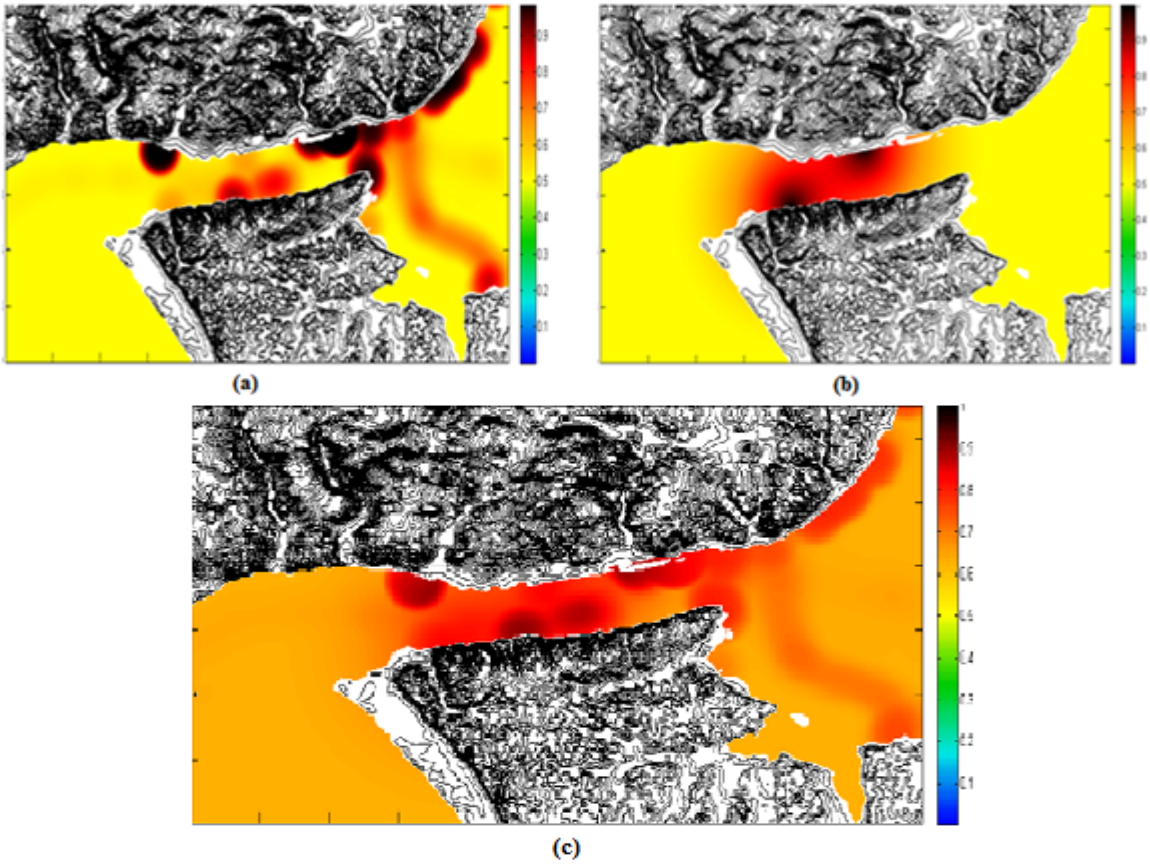


Figura 5.11 - Comparação do mapa de risco-base em (c) com a distribuição espacial do índice de Suscetibilidade em (a) e do índice de Criticidade em (b)

Prosseguindo a ilustração da metodologia, apresentamos dois mapas de risco residual na Figura 5.12 (a-b). Os mapas foram construídos a partir do mapa de risco-base representado pela Fig. 5.10(b) em duas situações: na Figura 5.12(a), o conjunto de índices de Ineficácia utilizado é o representado pela Figura 5.8(a) e na Figura 5.12(b), utilizamos o conjunto de índices de Ineficácia representado na Fig. 5.8(b).

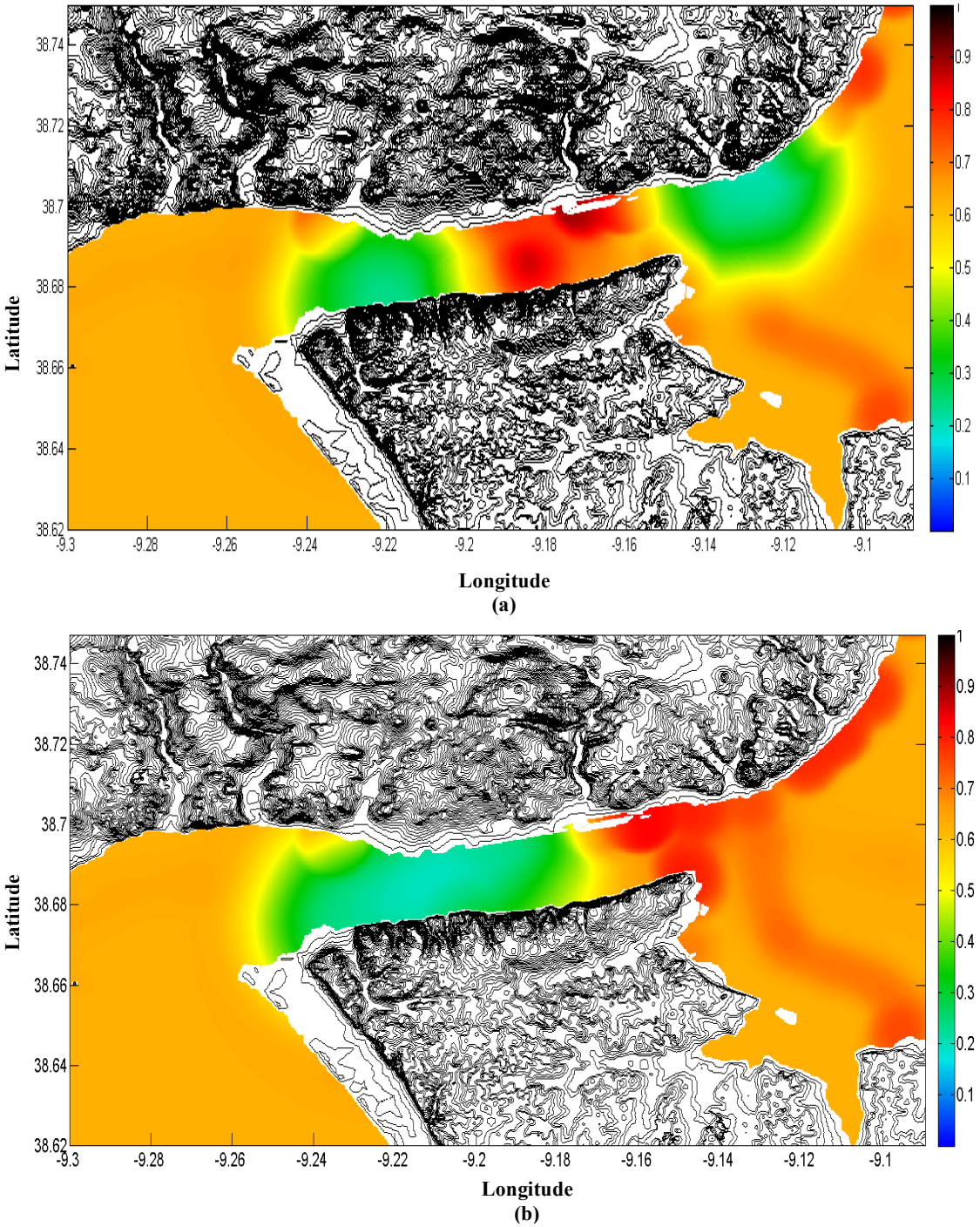


Figura 5.12 - Ilustrações do risco-residual de segurança espacial

A análise da Figura 5.12 (a-b) leva-nos às seguintes conclusões:

— Na Figura 5.12(a), permanecem pontos da área de interesse com altos índices de risco (SSRI) próximos ao ponto considerado crítico localizado na margem norte do rio Tejo;

— O ponto crítico localizado na margem Sul é coberto pelo sistema de proteção em qualquer situação avaliada, no entanto, o índice de risco não é reduzido a zero, está em torno de 0.3;

— A quantidade de pontos da AoI coberta pelos sistemas de proteção proposto é maior em (b) do que em (a).

6 CONCLUSÕES E PERSPETIVAS

Concluimos este trabalho com este capítulo, que está dividido em duas partes: na primeira, as principais conclusões são apresentadas e, na segunda, são propostas possíveis linhas de investigação para trabalhos futuros.

6.1 CONCLUSÕES

Estabelecer medidas de defesa contra ameaças terroristas coloca novos desafios e oportunidades para a avaliação de riscos. Os terroristas são modeláveis por variáveis adversariais que se adaptam às mudanças feitas pelos sistemas de proteção e decidem onde e quando atacar — opções que não estão disponíveis para gerir os riscos de desastres naturais ou de acidentes em parques industriais, por exemplo. Uma conclusão, óbvia, deste problema é que o risco não pode ser adequadamente refletido por, apenas, números que representem probabilidades interpretadas como a frequência de ocorrência de um evento.

Dessa forma, a principal proposta desta tese foi apresentar uma nova metodologia para avaliação de riscos denominada Risco de Segurança Espacial, que quase não dependesse de probabilidades, exceto as relacionadas com a definição do índice de Ineficácia. Contudo, tal como ilustrado, é por vezes possível e relevante incorporar uma análise frequencista de dados históricos na avaliação do índice de Suscetibilidade. Na metodologia, o risco é representado graficamente através de mapas, ou cartas bidimensionais, construídos a partir da agregação, por média geométrica, de 3 subíndices fundamentais, estimados para cada ponto da Área de Interesse.

Propusemos a elaboração de mapas de risco para permitir a visualização da distribuição do risco em termos espaciais. Esta abordagem propicia, pelo menos, duas importantes vantagens:

— Ajuda a prioritizar as zonas onde os recursos são mais necessários;
— Fornece uma forma de avaliação mais útil de uma potencial ineficácia residual de uma solução de proteção proposta.

Essas vantagens podem ser interpretadas como instrumentos para resolução eficiente de um problema de otimização, pois possibilita a avaliação e comparação de inúmeras possíveis soluções em várias fases de utilização de um sistema de apoio à decisão. Muitos problemas combinatórios são, frequentemente, abordados heuristicamente, utilizando-se de regras de sequenciamento que possibilitam a construção de soluções viáveis. Soluções obtidas heuristicamente são, geralmente, subótimas. Isto não significa que não sejam suficientemente próximas do "ótimo". No entanto, soluções ótimas são provavelmente impossíveis de se encontrar em períodos de tempo razoáveis em problemas como o aqui discutido, mesmo se forem utilizadas técnicas meta-heurísticas.

Métodos de pesquisa global, em particular, poderiam ajudar a resolver o problema de otimização, mas é conveniente conceber formas engenhosas de reduzir a enorme carga computacional, nomeadamente tendo em conta que certos aspetos dinâmicos — como a avaliação das capacidades de sensores móveis — podem exigir demoradas simulações. Argumentamos que um critério pessimista (minimax) para o risco e a minimização do custo devem ser considerados num problema de otimização dos recursos de defesa, a não ser que de antemão sejam introduzidas restrições pelos agentes de decisão, como, por exemplo, sobre o orçamento disponível ou sobre requisitos mínimos do sistema de proteção.

Tentámos esclarecer quais são os elementos essenciais de análise do risco onde alguns ingredientes na estimativa do índice de Risco de Segurança Espacial (*SSRI*) podem exigir mais ou menos esforços. De qualquer forma, as estimativas subjetivas são necessárias, mas devem ser obtidas de forma disciplinada por consulta a especialistas e aos decisores envolvidos. Por este motivo, decidimos definir os índices que compõem o risco de segurança espacial como utilidades, de forma a capturar os aspetos cognitivos e, principalmente, a atitude dos decisores perante o risco. Além disso, a existência de uma escala intervalar é um aspeto prático para avaliar o risco antes e depois da implementação dos recursos de defesa, definidos por um processo de otimização.

Ao se restringir o sistema em análise para um ambiente em que um ataque terrorista pode ser iniciado apenas por uma via, o mar, foi possível definir os diversos tipos de ameaças. Estas ameaças são interpretadas como variáveis adversariais, que influem na avaliação das 3 componentes de risco consideradas. Esta abordagem constitui uma inovação desta tese, uma vez que possibilitou que conceitos comummente utilizados num contexto de *safety risk* fossem adaptados à avaliação do risco de segurança contra o terrorismo, ou seja, num contexto de *security risk*. Isto permitiu que o problema fosse tratado como um processo de decisão sob incerteza parcial em oposição ao modo tradicional de tratá-lo como de incerteza aleatória. Alcançamos esse objetivo ao se abordar o problema de uma forma sistémica, inspirado no conceito de Avaliação Operacional, cujo objeto de avaliação compreende todo o espaço de interesse da infraestrutura crítica analisada, um porto, e as potenciais ameaças.

O índice de Suscetibilidade avalia o risco de segurança em todo o espaço da área considerada de interesse, sem ter em consideração os potenciais alvos ou os potenciais recursos de proteção. Contudo, a presença de uma ameaça próxima de um potencial alvo, acessível por via marítima, constitui um aspeto crítico que não seria capturado pelo índice de suscetibilidade. Sendo assim, foi definido o índice de Criticidade para refletir este aspeto da avaliação. Assim, temos uma forma hábil de fazer automaticamente a avaliação de qualquer situação — definida por um par (alternativa, *setting*) — com o objetivo de tentar "anular" o efeito combinado de suscetibilidade e criticidade e, associadamente, avaliar o risco residual.

Apesar da metodologia do risco de segurança no espaço ser baseada parcialmente em dados objetivos — isto é, de natureza física —, de forma a reduzir a incerteza da avaliação, tal não impede que seja feita uma avaliação subjetiva, complementar ou suplementar, por parte de um agente de decisão ou especialista. Durante a investigação, verificámos que uma administração portuária pode ser constituída por diferentes atores com autoridade para decidir sobre assuntos relacionados com a segurança. Com isso, nos deparamos com um problema de elicitação das opiniões e preferências de um grupo de decisores e, assim, o trabalho desenvolvido necessitou de ser expandido em outras direcções.

Fizemos uma proposta para lidar com o problema da elicitação de opiniões/preferências de um grupo, seja de decisores ou especialistas. A proposta, denominada Método Delphi Intervalar, foi apresentada no Capítulo 3 e constitui um protocolo formal, com base num método largamente experimentado para a elicitação de

opiniões e preferências de um grupo visando o levantamento de dados quantitativos sobre variáveis de interesse. Apesar de o Método Delphi Intervalar precisar de mais experiências para coleta de dados empíricos, acreditamos que constitui um procedimento útil para uso em painéis constituídos por especialistas heterogéneos em áreas multidisciplinares de interesse. Um aspeto importante derivado do método é a capacidade de proporcionar um processo analítico mais flexível para os decisores, pois possibilita que as estimativas sejam feitas sob a forma de intervalos. Estes intervalos viabilizam a estimação de uma função de densidade de probabilidade, sendo este um recurso importante na tomada de decisão, em particular por incluir informação sobre a incerteza que uma estimativa pontual não fornece.

Tendo em conta a necessidade de contornar a influência exagerada de que a opinião de um entrevistado ou de uma minoria de entrevistados poderia ter no processo de elicitação e agregação, foram consideradas alterações no clássico método do *kernel* para estimação (dita *não paramétrica*) de densidades. Sobretudo, considerámos a atribuição de diferentes pesos aos entrevistados, de forma a refletir a importância ou a credibilidade das opiniões e estimativas individuais. Esta abordagem pode prover uma forma de incentivo para os entrevistados reverem as suas opiniões, procurando ser mais úteis na obtenção de estimativas finais suficientemente consensuais. Contudo, gostaríamos de ressaltar que as propostas são baseadas em suposições feitas em processos de elicitação de um grupo. Elas não pretendem descrever como, de facto, o comportamento de um grupo interfere num processo de decisão; pretendem simplesmente opinar a respeito de certo nível da qualidade do processo no contexto do problema tratado neste trabalho — contexto onde as opiniões e as preferências do grupo podem estar envolvidas em incertezas, independentemente da experiência e conhecimento dos membros do painel Delphi.

Partimos do princípio que o comportamento perante o risco dos agentes envolvidos num processo de decisão para alocação dos recursos de proteção de um porto pode ser modelado por meio de uma função de utilidade exponencial. Entretanto, como estamos a lidar com as preferências de um grupo, verificamos que regras de agregação dessas funções encontradas na literatura possuem lacunas e podem não refletir alguma forma de consenso. Por isso, achamos que não seriam adequadas para o contexto do problema que tratamos. Desta forma, apresentamos no Capítulo 4 uma proposta de agregação de curvas utilidade exponenciais baseada na média geométrica dos parâmetros de aversão ao risco. Esta abordagem proporciona um forma automatizada e que permite a visualização da curva de aversão ao risco — recurso que, no mesmo raciocínio do método Delphi Intervalar, pode permitir aos agentes envolvidos reverem as suas opiniões.

Para terminar, refira-se que os estudos experimentais relacionados com o método Delphi Intervalar e a proposta de agregação de funções exponenciais foram realizadas através de interfaces originais e apropriadas, desenvolvidas na linguagem MATLAB.

6.2 PERSPETIVAS

Ao longo deste trabalho foram surgindo diversos desafios que deram origem a novas ideias que, por sua vez, proporcionam vias de investigação de teor bastante diverso. Pretendemos fazer agora uma sistematização de alguns tópicos que são considerados de maior interesse.

O planeamento de sistemas de proteção de portos e, até mesmo, outras infraestruturas consideradas críticas, especialmente contra ameaças terroristas, é um problema bastante complexo. Métodos de pesquisa metaheurística podem ajudar a resolver esse problema, contudo é conveniente conceber outras formas de reduzir o custo computacional geral, em particular, considerando uma abordagem de otimização de vários níveis e com a inclusão de métodos de otimização globais eficientes, baseados em superfícies de resposta.

Apesar do nosso estudo sobre elicitação de opiniões originar alguns resultados interessantes acerca das vantagens e desvantagens das aproximações que sugerimos, também tem algumas limitações que indicam a necessidade de investigação futura. Uma importante questão está relacionada com a atribuição da importância dos entrevistados através do método Delphi Intervalar: é necessário realizar muitos estudos empíricos para tentar saber quais dos procedimentos atrás descritos conduziria a melhores resultados. Tais experiências poderiam consistir na estimação subjetiva de quantidades cujos valores exatos pudessem ser posteriormente medidos ou conhecidos. Nessas experiências poderiam ser considerados não só diferentes procedimentos de ponderação, mas também diferentes critérios de terminação do processo, ou mesmo diferentes formas de entender o grau de certeza associado a uma estimativa intervalar. Concretamente, é legítimo pensar que 90% é um valor apropriado na primeira ronda mas, nas rondas seguintes, os entrevistados poderão querer afirmar convicções mais fortes — isto é, com menor incerteza mas não necessariamente com menor erro — através das suas estimativas intervalares.

Uma mesma linha de raciocínio poderia ser seguida para a avaliação da proposta de agregação de funções de utilidade num grupo, ou seja, procedimentos empíricos precisam ser realizados para testar a eficácia do método proposto. Experiências poderiam

ser feitas em estudos de casos reais, comparando a proposta apresentada com métodos descritos na Secção 4.5.

Uma forma para aumentar a eficiência de aplicação do método Delphi é o seu uso através de um *web browser*, em especial na versão conhecida como *Real-time Delphi* (Gordon e Pease, 2006). Portanto, o desenvolvimento de uma aplicação *web* para o método Delphi Intervalar será um caminho natural a seguir.

REFERÊNCIAS BIBLIOGRÁFICAS

Abrahms, M. What terrorists really want: Terrorist motives and counterterrorism strategy. **International Security**, 2008, 32(4), 78-105.

Al Mannai, W.I. **Development of a Decision Support Tool to Inform Resource Allocation for Critical Infrastructure Protection in Homeland Security**. Tese de doutoramento, Naval Postgraduate School, Monterey, CA, EUA, 2008.

Apostolakis, G.E.; Lemon, D.M.A. A Screening methodology for the identification and ranking of infrastructure vulnerabilities due to terrorism. **Risk Analysis**, 2005, 25(2), 361-376.

Arrow, K. **Social Shoice and Individual Values**. Wiley, 1951.

Aven, T. A unified framework for risk and vulnerability analysis covering both safety and security. **Reliability Engineering & System Safety**, 2007, 92(6), 745-754.

_____. Risk analysis and management. Basic concepts and principles. **Reliability & Risk Analysis**, 2009a, 4(1), 57-73.

_____. The role of quantitative risk assessments for characterizing risk and uncertainty and delineating appropriate risk management options, with special emphasis on terrorism. **Risk Analysis**, 2009b, 29(4), 587-600.

_____. **Misconceptions of Risk**. Wiley, 2010.

Ayyub, B.M. Elicitation of Expert Opinions for Uncertainty and Risks, CRC Press, 2001.

Bakken, B. **Handbook on Long Term Defence Planning**. Technical Report RTO-TR-069, NATO Research and Technology Organisation, 2003.

Belton, V.; Stewart, T. **Multiple Criteria Decision Analysis: an Integrated Approach**. Springer, 2002.

Berbash, K. **A Risk-Based Optimization Framework for Security Systems Upgrades at Airports**. Tese de doutoramento, University of Warteloo, Canadá, 2010.

Bernoulli, D. Exposition of a new theory on the measurement of risk, *Comentarii Academiae Scientiarum Imperialis Petropolitanae*, 1738. Traduzido e reimpresso em: **Econometrica**, 1954, 22, 23-36.

Bhashyam, S.S.; Montibeller, G. Modeling state-dependent priorities of malicious agents. **Decision Analysis**, 2012, 9(2), 172–185.

Bier, V.; Oliveros, S.; Samuelson, L. Choosing what to protect: Strategic defensive allocation against an unknown attacker. **Journal of Public Economic Theory**, 2007, 9(4), 563–587.

Bordley, R.; Licalzi, M. Decision analysis using targets instead of utility functions. **Decisions in Economics and Finance**, 2000, 23(1), 53-74.

Bose, U.; Davey, A.M.; Olson, D.L. Multi-attribute utility methods in group decision making: Past applications and potential for inclusion in GDSS. **Omega**, 1997, 25(6), 691-706.

Brown, G.C.; Carlyle, M.; Abdul-Ghaffar, A.; Kline, J. A defender-attacker optimization of port radar surveillance. **Naval Research Logistics**, 2011, 58(3), 223-235.

Brown, G.C.; Cox, L.A. How probabilistic risk assessment can mislead terrorism risk analysts. **Risk Analysis**, 2011, 31(2), 196–204.

Butler, J.C.; Merrick, J.R.; Morrice, D.J. Assessing oil spill risk in port tanker operations using a multiattribute utility approach to ranking and selection. **Proceedings of the 2011 Winter Simulation Conference**, Institute of Electrical and Electronics Engineers, 2011, 1696-1707.

Caiti, A.; Munafò, A.; Vettori, G.A. A Geographical Information System (GIS)-based simulation tool to assess civilian harbor protection levels. **IEEE Journal of Oceanic Engineering**, 2012, 37(1), 85-102.

Carmo, J.L.N. **Previsão da Procura e Decisão Optimal: Modelos e Métodos Avançados**. Tese de doutoramento, Faculdade de Ciências da Universidade de Lisboa, 2007.

Carvalho, A.S.F. **Algoritmo Genético para o Problema de Localização de Sensores**. Tese de mestrado, Faculdade de Ciências da Universidade de Lisboa, 2013.

Chung, H.; Polak, E.; Royset, J.O.; Sastry, S. On the optimal detection of an underwater intruder in a channel using unmanned underwater vehicles. **Naval Research Logistics**, 2011, 58(8), 804-820.

Cooke, R.M.; Goossens, L. Expert judgement elicitation for risk assessments of critical infrastructures. **Journal of Risk Research**, 2004, 7(6), 643-656.

Cooke, R.M. **Experts in uncertainty: opinion and subjective probability in science**. Oxford University Press, 1991.

Cox, Jr., L.A. What´s wrong with risk matrices? **Risk Analysis**, 2008, 28(2), 497-512.

_____. Game Theory and Risk Analysis. **Risk Analysis**, 2009a, 29(8), 1062-1068.

_____. **Risk Analysis of Complex and Uncertain Systems**. Springer, 2009b.

_____. Confronting deep uncertainties in risk analysis. **Risk Analysis**, 2012, 32(10), 1607-1629.

Degrassi, S. **The Seaport Network Hamburg**. Tese de doutoramento, Universität Hamburg, Alemanha, 2001.

Dias, L.C. **A Informação Imprecisa e os Modelos Multicritério de Apoio à Decisão – Identificação e Uso de Conclusões Robustas**. Tese de doutoramento, Faculdade de Economia da Universidade de Coimbra, 2000.

Dias, L.C.; Sarabando, P. A note on a group preference axiomatization with cardinal utility. **Decision Analysis**, 2012, 9(3), 231-237.

Dias, L.C.; Tsoukiàs, A. On the constructive and other approaches in decision aiding. In: C.H. Antunes, J. Figueira, J. Clímaco (eds), **Aide Multicritére à la Décision: Multiple Criteria Decision Aiding**, 13-28. CCDRC/INESCC/FEUC, Coimbra, 2004.

Dillon, R.L.; Liebe, R.M.; Bestafka, T. Risk-based decision making for terrorism applications. **Risk Analysis**, 2009, 29(3), 321-335.

Doise, W. Intergroup relations and polarization in individual and collective judgements. **Journal of Personality and Social Psychology**, 1969, 12, 136-143.

Edwards, W.; Winterfeldt, D.; Moody, D.L. Simplicity in decision analysis: an example and a discussion. In: D.E. Bell, H. Raiffa, A. Tversky (eds.), **Decision making: Descriptive, Normative and Prescriptive Interactions**, Cambridge University Press, 1988, 443–464.

Ellingsen, S.A. **Nuclear Terrorism and Rational Choice**. Tese de doutoramento, King's College London, R.U., 2009.

Estado-Maior da Armada. **EMA-333, Sistemática para Avaliação Operacional na Marinha do Brasil**, Brasília, DF, Brasil, 2004.

Farquhar, P.H. State of the art — Utility assessment methods. **Management Science**, 1984, 30(11), 1283-1300.

Fleming, P.J., Wallace, J.J. How not to lie with statistics: the correct way to summarize benchmark results. **Communications of the ACM**, 1986, 29(3), 218-221.

French, S. **Decision Theory: An Introduction to the Mathematics of Rationality**. Halsted Press, 1986.

Galway, L.A. **Subjective Probability Distribution Elicitation in Cost Risk Analysis: A Review**. RAND Corporation, 2007.

Garrick, B.; Hall, J. E.; Kilger, M.; McDonald, J.C.; O'Toole, T.; Probst, P.S.; Zebroski, E.L. Confronting the risks of terrorism: Making the right decisions. **Reliability Engineering & System Safety**, 2004, 86(2), 129-176.

Garthwaite, P.H.; Kadane, J. B.; O'Hagan, A. Statistical methods for eliciting probability distributions. **Journal of the American Statistical Association**, 2005, 100(470), 680-701.

Ghafoori, A. **Decision Analytics for Sonar Placement to Mitigate Maritime Security Risk**. Tese de doutoramento, The State University of New Jersey, 2013.

Giadrosich, D.L. **Operations Research Analysis in Test and Evaluation**. American Institute of Aeronautics and Astronautics, Washington, DC, EUA, 1995.

Gilovich, T; Griffin, D; Kahneman, D. **Heuristics and Biases: The Psychology of Intuitive Judgment**. Cambridge University Press, 2002.

Goetz, S.J.; Deller, S.D.; Harris, T.R. (eds.). **Targeting Regional Economic Development**. Routledge, 2009.

Goodwin, P.; Wright, G. **Decision Analysis for Management Judgment**. Wiley, 1998.

Gordon, T.; Pease, A. RT Delphi: an efficient, "round-less" almost real time Delphi method. **Technological Forecasting and Social Change**, 2006, 73(4), 321-333.

Gouldby, B.; Sayers, P.; Mulet-Marti, J.; Hassan, M.A.A.M.; Benwell, D. A methodology for regional-scale flood risk assessment. **Proceedings of the ICE-Water Management**, 2008, 161(3), 169-182.

Greenberg, M.R. Risk analysis and port security: Some contextual observations and considerations. **Annals of Operations Research,** 2011, 187(1), 121-136.

Haimes, Y.Y. On the complex definition of risk: A systems-based approach. **Risk Analysis,** 2009, 29(12), 1647-1654.

Hämäläinen, R.P.; Kettunen, E.; Marttunen, M.; Ehtamo, H. Evaluating a framework for multi-stakeholder decision support in water resources management. **Group Decision and Negotiation**, 2001, 10(4), 331-353.

Hämäläinen, R.P.; Lindstedt, M.R.; Sinkko, K. Multiattribute risk analysis in nuclear emergency management. **Risk Analysis**, 2000, 20(4), 455-468.

Hora, S. Eliciting probabilities from experts. In: W. Edwards, R.F. Miles, Jr., D. von Winterfeldt (eds.) **Advances in Decision Analysis: From Foundations to Applications**, Cambridge University Press, 2007, 129-153.

Hubbard, D.; Evans, D. Problems with scoring methods and ordinal scales in risk assessment. **IBM Journal of Research and Development**, 2010, 54(3), 2:1-2:10.

IMO, **ISPS Code - 2003 Edition**, International Maritime Organization, London. 2003.

Jiménez, A.; Ríos-Insua, S.; Mateos, A. A decision support system for multiattribute utility evaluation based on imprecise assignments. **Decision Support Systems**, 2003, 36, 65-79.

Kaplan, S.; Garrick, B.J. On the quantitative definition of risk. **Risk Analysis**, 1981, 1(1), 11-27.

Keeney, R.L. A group preference axiomatization with cardinal utility. **Management Science**, 1976, 23(2), 140–145.

_____. Common mistakes in making value trade-offs. **Operations Research**, 2002, 935-945.

_____. Developing objectives and attributes. In: W. Edwards, R.F. Miles, D. von Winterfeldt, (eds.), **Advances in Decision Analysis: From Foundations to Applications**, 2007, 104-128.

_____. **Value-Focused Thinking: A Path to Creative Decisionmaking**. Harvard University Press, 2009.

_____. Foundations for group decision analysis. **Decision Analysis**, 2013, 10(2), 103-120.

Keeney, R.L.; Kirkwood, C.W. Group decision making using cardinal social welfare functions. **Management Science**, 1975, 22(4), 430-437.

Keeney, R.L.; Raiffa, H. **Decisions With Multiple Objectives**. Cambridge University Press, New York, 1976. Republicado por Cambridge University Press, Cambridge, 1993.

Keeney, R.L.; Gregory, R.S. Selecting attributes to measure the achievement of objectives. **Operations Research**, 2005, 53(1), 1-11.

Keeney, G.L.; Winterfeldt, D. von W. Identifying and structuring the objectives of terrorists. **Risk Analysis**, 2010, 30(12), 1803-1816.

_____. A value model for evaluating homeland security decisions. **Risk Analysis,** 2011, 31(9), 1470 – 1487.

Kharroubi, S.A.; Brazier, J.E.; McGhee, S. Modeling SF-6D Hong Kong standard gamble health state preference data using a nonparametric Bayesian method, **Value in Health**, 2013, 16(6), 1032-1045.

Leitch, M. ISO 31000:2009 - The new international standard on risk management. **Risk Analysis**, 2010, 30(6), 887-892.

Leung, M.; Lambert, J.H.; Mosenthal, A. A risk-based approach to setting priorities in protecting bridges against terrorist attacks. **Risk Analysis**, 2004, 24(4), 963-984.

Lewis, T.G. **Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation**. Wiley, 2006.

Lichtenstein, S; Slovic, P. (eds.) **The Construction of Preference**. Cambridge University Press, 2006.

Lin, S.W.; Bier, V.M. A study of expert overconfidence. **Reliability Engineering & System Safety**, 2008, 93(5), 711-721.

Lindell, M.K; Prater, C.S. Assessing community impacts of natural disasters. **Natural Hazards Review**, 2003, 4(4), 176-185.

Linstone, H.A.; Turoff, M. (eds.) **The Delphi Method: Techniques and Applications**. New Jersey Institute of Technology, NJ, EUA, 2002.

Lucas, T.W. Damage functions and estimates of fratricide and collateral damage. **Naval Research Logistics**, 2003, 50(4), 306-321.

Lundberg, R. **Comparing Homeland Security Risks Using a Deliberative Risk Ranking Methodology**. Tese de doutoramento, Pardee RAND Graduate School, 2013.

Mahafza, B.R. **Radar Systems Analysis and Design Using MATLAB**. Chapman and Hall, New York, 2002.

Martins, M.; Casimiro, R.P.; Gonçalves, S.; Calado, J.; Manso, M.; Lopes, J.; Rodrigues, A.; Captivo, M.E.; Freitas, J.C.; Abreu, M.A.; Gonçalves, G.; Sousa, J.; Bezzeghoud, M.; Salgado, R. The SAFE-PORT Project: An approach to port surveillance and protection. In: **Proceedings of WSS 2010 – 2nd International Conference on Waterside Security**, NURC (NATO), 2010.

Maslow, A.H. **Motivation and Personality, 3rd ed..** Harper & Row, 1970.

Masse, T.; O'Neil, S.; Rollins, J. **The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress**. Library of Congress, Washington DC, 2007.

McCarthy, J.J.; Canziani, O.F.; Leary, N.A.; Dokken, D.J.; White, K.S. (eds.). **Climate Change 2001: Impacts, Adaptation, and Vulnerability.** Cambridge University Press, 2001.

McGill, W.L.; Ayyub, B.M.; Kaminskiy, M. Risk analysis for critical asset protection. **Risk Analysis**, 2007, 27(5), 1265-1281.

Mileti, D. **Disasters by Design: A Reassessment of Natural Hazards in the United States**. Joseph Henry Press, 1999.

Moder, J.J.; Rodgers, E.G. Judgment estimates of the moments of PERT type distributions. **Management Science**, 1968, 15(2), B-76-B-83.

Morgan, M.G.; Henrion, M. **Uncertainty: A Guide to Dealing with Uncertainty in Quantitative Risk and Policy Analysis**. Cambridge University Press, 1992.

Moscovici, S.; Doise, W.; Dulong, R. Studies in group decision II: Differences of positions, differences of opinion and group polarization. **European Journal of Social Psychology**, 1972, 2(4), 385-399

Mun, J. **Applied Risk Analysis: Moving Beyond Uncertainty in Business**. Wiley, 2004.

Myagmar, S.; Lee, A.J.; Yurcik, W. Threat modeling as a basis for security requirements. **Symposium on Requirements Engineering for Information Security (SREIS)**, 2005.

Myerson, R.B. **Fundamentals of Social Choice Theory**. Discussion Paper No. 1162, CMS-EMS, Northwestern University, EUA, 1996.

Naamani-Dery, L.; Golan, I.; Kalech, M.; Rokach, L. Preference elicitation for group decisions using the Borda voting rule. **Group Decision and Negotiation**, 2015, 1-19.

Nakayama, H.; Tanino, T.; Matsumoto, K.; Matsuo, H.; Inoue, K.; Sawaragi, Y. Methodology for group decision support with an application to assessment of residential environment. **IEEE Transactions on Systems, Man, and Cybernetics**, 1979, 9(9), 447–485.

NATO Standardization Agency. **AAP – 6, NATO Glossary of Terms and Definitions of Military Significance for use in NATO (English and French)**, 2011.

Ness, J.; Hoffman, C. **Putting Sense into Consensus: Solving the Puzzle of Making Team Decisions**. VISTA Associates, 1998.

O'Hagan, A.; Buck, C.E.; Daneshkhah, A.; Eiser, J.R.; Garthwaite, P.H.; Jenkinson, D.J; Oakley, J.E.; Rakow, T. **Uncertain Judgements: Eliciting Experts' Probabilities**. Wiley, 2006.

Parenté, R.J.; Hiöb, T.N.; Silver, R.A.; Jenkins, C.; Poe, M.P.; Mullins, R.J. The Delphi method, impeachment and terrorism: Accuracies of short-range forecasts for volatile world events. **Technological Forecasting and Social Change**, 2005, 72(4), 401-411.

Parfomak, P.W.; Fritelli, J. **Maritime Security: Potencial Terrorist Attacks and Protection Priorities**. Library of Congress Washington DC, EUA, 2007.

Parkin, R.T.; Balbus, J.M. Variations in concepts of "susceptibility" in risk assessment. **Risk Analysis**, 2000, 20(5), 603-612.

Paté-Cornell, M.E. Uncertainties in risk analysis: Six levels of treatment. **Reliability Engineering & System Safety**, 1996, 54(2-3), 95-111.

_____. Risk and uncertainty analysis in government safety decisions. **Risk Analysis**, 2002, 22(3), 633-646.

Paté-Cornell, M.E.; Guikema, S. Probabilistic modeling of terrorist threats: A systems analysis approach to setting priorities among countermeasures. **Military Operations Research**, 2002, 7(4), 5-20.

Pattanaik, P.K. Social welfare function. In: S.N. Durlauf; L.E. Blume (eds.) **The New Palgrave Dictionary of Economics**, **2nd Ed.** Palgrave Macmillan, 2008, 955-958.

Raaijmakers, R.; Krywkow, J.; Van der Veen, A. Flood risk perceptions and spatial multi-criteria analysis: An exploratory research for hazard mitigation. **Natural Hazards**, 2008, 46(3), 307-322.

Radu, O.; Slămnoiu, G.; Zărnescu, L.; Coşereanu, L. Harbor protection against terrorist threats: Difficulties and possible solutions. **Proceedings of the NATO RTO System Concept and Integration (SCI) Panel Symposium on Force Protection in the Littorals**, RTO-MP-SCI-180, 2006.

Rauch, W. The Decision Delphi. **Technological Forecasting and Social Change**, 1979, 15(3), 159-169.

Reifel, C.S. **Quantitative Risk Analysis for Homeland Security Resource Allocation**. Tese de mestrado, Naval Postgraduate School, Monterey,CA, EUA, 2006.

Resnyansky, L. Conceptualisation of terrorism in modelling tools: Critical reflexive approach. **Prometheus**, 2006, 24(4), 441-447.

Richards, M.G. **Multi-Attribute Tradespace Exploration for Survivability**. Tese de doutoramento, Massachusetts Institute of Technology, 2009.

Rodrigues, A.J.R. Minimizing port security risk. **Proceedings of the NATO RTO SCI-247 Symposium on Port and Regional Maritime Security**, 2012.

Rosoff, H.B. **Using Decision and Risk Analysis to Assist in Policy Making about Terrorism**. Tese de doutoramento, University of Southern California, EUA, 2009.

Salo, A. Interactive decision aiding for group decision support. **European Journal of Operational Research**, 1995, 84(1), 134–149.

Sarabando, P.C. **Escolha e Ordenação com Informação Ordinal: Extensão à Decisão em Grupo e à Negociação.** Tese de doutoramento, Faculdade de Economia da Universidade de Coimbra, 2010.

Savage, L.J. **The Foundation of Statistics**, Wiley, 1954.

Scouras, J.; Parnell, G.S.; Ayyub, B.M.; Liebe, R.M. Risk analysis frameworks for counterterrorism. **Wiley Handbook of Science and Technology for Homeland Security**, 2009.

Silva, D.F.M.F. **Heurísticas para Localização de Sensores**. Tese de mestrado, Faculdade de Ciências da Universidade de Lisboa, 2013.

Silva, P.A.R. **Proteção Portuária em Ambiente de Anti-Terrorismo**. Instituto de Estudos Superiores Militares, Lisboa, 2011.

Silverman, B.W. **Density Estimation for Statistics and Data Analysis**. CRC Press, 1986.

Simonson, I. Will I like a "medium" pillow ? Another look at constructed and inherent preferences. **Journal of Consumer Psychology**, 2008, 18(3), 155-169.

Slottje, P.; van der Sluijs, J.P.; Knol, A.B. **Expert Elicitation: Methodological Suggestions for its Use in Environmental Health Impact Assessments**. RIVM Letter report 630004001/2008, National Institute for Public Health and the Environment, Holanda, 2008.

Slovic, P. Perception of risk: Reflections on the psychometric paradigm. In S. Krimsky & D. Golding (Eds.), **Social Theories of Risk**, 1992, 117-152.

Slovic, P. Terrorism as hazard: a new species of trouble. **Risk Analysis**, 2002, 22(3), 425-426.

Slovic, P.; Weber, E.U. **Perception of Risk Posed by Extreme Events**. Center for Decision Sciences, Columbia University, EUA, 2002.

Soll, J.B.; Klayman, J. Overconfidence in interval estimates. **Journal of Experimental Psychology: Learning, Memory, and Cognition**, 2004, 30(2), 299.

Speirs‐Bridge, A.; Fidler, F.; McBride, M.; Flander, L.; Cumming, G.; Burgman, M. Reducing overconfidence in the interval judgments of experts. **Risk Analysis**, 2010, 30(3), 512-523.

Stevens, S.S. On the theory of scales of measurement. Science, 1946, 103(2684), 677-680.

Stewart, T.J. Simplified approaches for multicriteria decision making under uncertainty. **Journal of Multi-Criteria Decision Analysis**, 1995, 44(4), 246–258.

Teigen, K.H.; Jørgensen, M. When 90% confidence intervals are 50% certain: on the credibility of credible intervals. **Applied Cognitive Psychology**, 2005, 19(4), 455-475.

Teixeira, L.S.; Rodrigues, A.J.L. Avaliação de riscos na proteção de portos. **Jornadas do Mar**, Escola Naval, 2012.

Tetlock, P. **Expert Political Judgment: How Good Is It? How Can We Know?** Princeton University Press, 2005.

Torrance, G.W. Measurement of health state utilities for economic appraisal: a review. **Journal of Health Economics**, 1986, 5(1), 1-30.

Trainor, T.E.; Parnell, G.S.; Kwinn, B.; Brence, J.; Tollefson, E.; Downes, P. The US army uses decision analysis in designing its US installation regions. **Interfaces**, 2007, 37(3), 253-264.

Tsai, C.I.; Klayman, J.; Hastie, R. Effects of amount of information on judgment accuracy and confidence. **Organizational Behavior and Human Decision Processes**, 2008, 107(2), 97-105.

Tversky, A.; Kahneman, D. Judgment under uncertainty: Heuristics and biases. **Science**, 1974, 185(4157), 1124-1131.

Tzannatos, E. A decision support system for the promotion of security in shipping. **Disaster Prevention and Management**, 2003, 12(3), 222-229.

US-DHS. **National Infrastructure Protection Plan.** The U.S. Department of Homeland Security, EUA, 2009.

US-DoD. **Mandatory Procedures for Major Defense Acquisitions Programs (MDAPS) and Major Automated Information System (MAIS) Acquisition Programs**. DoD Regulation 5000.2-R, Washington, DC, EUA, 2002.

US-GAO. **Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure**. Report to Congressional Requesters GAO-06-91, EUA, 2005.

Van der Linde, E.; Van der Duin, P. The Delphi method as early warning: Linking global societal trends to future radicalization and terrorism in The Netherlands. **Technological Forecasting and Social Change**, 2011, 78(9), 1557-1564.

Verde, J.; Zêzere, J.L. Avaliação da perigosidade de incêndio florestal. **Actas do VI Congresso da Geografia Portuguesa**, Lisboa, 2007.

Von der Gracht, H.A. Consensus measurement in Delphi studies: Review and implications for future quality assurance. **Technological Forecasting and Social Change**, 2012, 79(8), 1525-1536.

Von Neumann, L.J.; Morgenstern, O. **Theory of Games and Economic Behavior**, 2nd ed., Princeton University Press. 1947.

Vroom, V.H. **Work and Motivation**, Wiley, 1964.

Wagner, D.H.; Mylander, W.C.; Sanders, T.J. (eds.) **Naval Operations Analysis**, 3rd ed. Naval Institute Press, 1999.

Wakker, P.; Deneffe, D. Eliciting von Neumann-Morgenstern utilities when probabilities are distorted or unknown. **Management Science**, 1996, 42(8), 1131-1150.

Wang, C.; Bier, V.M. Target-hardening decisions based on uncertain multiattribute terrorist utility. **Decision Analysis**, 2011, 8(4), 286-302.

Warren, C.; McGraw, A.P.; Van Boven, L. Values and preferences: defining preference construction. **Wiley Interdisciplinary Reviews: Cognitive Science**, 2011, 2(2), 193-205.

Washburn, A.R. **Notes on Firing Theory**. Naval Postgraduate School, Monterey, CA, EUA, 2000.

_____. **Search and Detection**. Institute for Operations Research and the Management Sciences, 2002.

Weil, R.; Apostolakis, G.E. A methodology for the prioritization of operating experience in nuclear power plants. **Reliability Engineering & System Safety**, 2001, 74(1), 23-42.

White III, C.C.; Holloway, H.A. Resolvability for imprecise multiattribute alternative selection. **IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans**, 2008, 38(1), 162-169.

Willis, H.H.; DeKay, M.L.; Morgan, M.G.; Florig, H.K.; Fischbeck, P.S. Ecological risk ranking: Development and evaluation of a method for improving public participation in environmental decision making. **Risk Analysis**, 2004, 24(2), 363-378.

Willis, H.H. Guiding resource allocations based on terrorism risk. **Risk Analysis**, 2007, 27(3), 597-606.

Wilson, J.L. **Advancements in the Elicitation, Aggregation, and Forecasting of Probability Distributions under Time Constraints**. Tese de doutoramento, San Diego State University, 2013.

Winkler, R.L. Combining probability distributions from dependent information sources. **Management Science**, 1981, 27(4), 479-488.

Winterfeldt, D.V.; Edwards, W. **Decision Analysis and Behavioral Research**. Cambridge University Press, 1986.

Wu, Q.; Rao, N.S.V.; Du, X.; Iyengar, S.S.; Vaishnavi, V.K. On efficient deployment of sensors on planar grid. **Computer Communications**, 2007, 30(14-15), 2721-2734.

Xu, Y.; Low, M.Y.H.; Choo, C.S. Enhancing automated red teaming with evolvable simulation. **Proceedings of the First ACM/SIGEVO Summit on Genetic and Evolutionary Computation**, ACM, 2009, 687-694.

Zajonc, R.B. Feeling and thinking: Preferences need no inferences. **American Psychologist**, 1980, 35(2), 151.